

ZyAIR G-2000 Plus

802.11g Wireless 4-port Router

User's Guide

Version 3.60
12/2004



Copyright

Copyright © 2004 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

Go to www.zyxel.com

- 1 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 2 Select the certification you wish to view from this page

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

- 1** To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
- 2** Do not use this product near water, for example, in a wet basement or near a swimming pool.
- 3** Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
WORLDWIDE	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		
FINLAND	support@zyxel.fi	+358 9 4780 8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358 9 4780 8448		

a. “+” is the (prefix) number you enter to make an international telephone call.

Table of Contents

Copyright	2
Federal Communications Commission (FCC) Interference Statement	3
ZyXEL Limited Warranty	4
Customer Support.....	5
Preface	32
Chapter 1	
Getting to Know Your ZyAIR	36
1.1 Introducing the ZyAIR	36
1.2 ZyAIR Features	36
1.2.1 Physical Features	36
1.2.1.1 4-Port Switch	36
1.2.1.2 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface	36
1.2.1.3 10/100M Auto-crossover Ethernet/Fast Ethernet Interface	36
1.2.1.4 10/100 Mbps Ethernet WAN	37
1.2.1.5 Reset Button	37
1.2.1.6 ZyAIR LED	37
1.2.2 Firmware Features	37
1.2.2.1 Internal RADIUS Server	37
1.2.2.2 Wi-Fi Protected Access	37
1.2.2.3 802.11b Wireless LAN Standard	37
1.2.2.4 802.11g Wireless LAN Standard	38
1.2.2.5 STP (Spanning Tree Protocol) / RSTP (Rapid STP)	38
1.2.2.6 Certificates	38
1.2.2.7 Limit the number of Client Connections	38
1.2.2.8 SSL Passthrough	38
1.2.2.9 Firewall	39
1.2.2.10 Brute-Force Password Guessing Protection	39
1.2.2.11 Wireless LAN MAC Address Filtering	39
1.2.2.12 WEP Encryption	39
1.2.2.13 IEEE 802.1X Network Security	39
1.2.2.14 Universal Plug and Play (UPnP)	39
1.2.2.15 Dynamic DNS Support	39

1.2.2.16 PPPoE Support (RFC2516)	40
1.2.2.17 PPTP Encapsulation	40
1.2.2.18 Network Address Translation (NAT)	40
1.2.2.19 Traffic Redirect	40
1.2.2.20 NAT for Single-IP-address Internet Access	40
1.2.2.21 DHCP (Dynamic Host Configuration Protocol)	40
1.2.2.22 Multicast	41
1.2.2.23 IP Alias	41
1.2.2.24 IP Policy Routing	41
1.2.2.25 SNMP	41
1.2.2.26 Full Network Management	41
1.2.2.27 Logging and Tracing	41
1.2.2.28 Diagnostics Capabilities	41
1.2.2.29 Embedded FTP and TFTP Servers	42
1.2.2.30 Wireless Association List	42
1.2.2.31 Wireless LAN Channel Usage	42
1.3 Applications for the ZyAIR	42
1.3.1 Internet Access Application	42
Chapter 2	
Introducing the Web Configurator.....	44
2.1 Web Configurator Overview	44
2.2 Accessing the ZyAIR Web Configurator	44
2.3 Resetting the ZyAIR	46
2.3.1 .Procedure To Use The Reset Button	46
2.3.2 Method of Restoring Factory-Defaults Via Web Configurator	46
2.4 Navigating the ZyAIR Web Configurator	46
Chapter 3	
Wizard Setup	48
3.1 Wizard Setup Overview	48
3.1.1 Channel	48
3.1.2 ESS ID	48
3.1.3 WEP Encryption	48
3.1.4 WPA-PSK	49
3.2 Wizard Setup: General Setup	49
3.3 Wizard Setup: Wireless LAN	50
3.4 Wizard Setup: Screen 3	51
3.5 Wizard Setup: Screen 4	53
3.5.1 Ethernet	53
3.5.2 PPPoE Encapsulation	55
3.5.3 PPTP Encapsulation	56
3.6 Wizard Setup: Screen 5	58

3.6.1 WAN IP Address Assignment	58
3.6.2 IP Address and Subnet Mask	59
3.6.3 DNS Server Address Assignment	59
3.6.4 WAN MAC Address	59
3.7 Basic Setup Complete	62
Chapter 4	
System Screens	64
4.1 System Overview	64
4.2 Configuring General Setup	64
4.3 Dynamic DNS	65
4.3.1 DynDNS Wildcard	65
4.4 Configuring Dynamic DNS	66
4.5 Configuring Password	67
4.6 Configuring Time Setting	68
Chapter 5	
LAN Screens	70
5.1 LAN Overview	70
5.2 DHCP Setup	70
5.2.1 IP Pool Setup	70
5.2.2 System DNS Servers	70
5.3 LAN TCP/IP	70
5.3.1 Factory LAN Defaults	70
5.3.2 IP Address and Subnet Mask	71
5.3.3 RIP Setup	71
5.3.4 Multicast	71
5.4 Configuring IP	72
5.5 Configuring Static DHCP	75
5.6 Configuring IP Alias	76
Chapter 6	
Wireless Configuration and Roaming	78
6.1 Wireless LAN Overview	78
6.1.1 IBSS	78
6.1.2 BSS	78
6.1.3 ESS	79
6.2 Wireless LAN Basics	80
6.2.1 RTS/CTS	80
6.2.2 Fragmentation Threshold	81
6.3 Configuring Wireless	82
6.4 Configuring Roaming	84
6.4.1 Requirements for Roaming	85

Chapter 7	
Wireless Security	88
7.1 Wireless Security Overview	88
7.2 Security Parameters Summary	90
7.3 WEP Overview	90
7.3.1 Data Encryption	90
7.3.1.1 Authentication	90
7.4 Configuring WEP Encryption	91
7.5 Introduction to WPA	93
7.5.1 User Authentication	93
7.5.2 Encryption	94
7.5.3 WPA-PSK Application Example	94
7.6 Configuring WPA-PSK Authentication	95
7.7 Wireless Client WPA Supplicants	97
7.7.1 WPA with RADIUS Application Example	97
7.8 Configuring WPA Authentication	98
7.9 Introduction to RADIUS	100
7.9.1 Types of RADIUS Messages	100
7.9.1.1 Access-Challenge	100
7.9.1.2 Accounting-Request	101
7.9.1.3 Accounting-Response	101
7.9.1.4 EAP Authentication Overview	101
7.10 Configuring RADIUS	102
7.11 802.1x Overview	104
7.12 Dynamic WEP Key Exchange	104
7.13 Configuring 802.1x and Dynamic WEP Key Exchange	105
7.14 Configuring 802.1x and Static WEP Key Exchange	107
7.15 Configuring 802.1x	110
7.16 MAC Filter	112
 Chapter 8	
Internal RADIUS Server	114
8.1 Internal RADIUS Overview	114
8.2 Internal RADIUS Server Setting	116
8.3 Trusted AP Overview	118
8.4 Configuring Trusted AP	119
8.5 Trusted Users Overview	120
8.6 Configuring Trusted Users	120
 Chapter 9	
WAN	124
9.1 WAN Overview	124
9.2 Configuring WAN ISP	124

9.2.1 Ethernet Encapsulation	124
9.2.1.1 Service Type	125
9.2.2 PPPoE Encapsulation	126
9.2.3 PPTP Encapsulation	129
9.3 TCP/IP Priority (Metric)	131
9.4 Configuring WAN IP	131
9.5 Configuring WAN MAC	134

Chapter 10

Single User Account (SUA) / Network Address Translation (NAT)..... 136

10.1 NAT Overview	136
10.1.1 NAT Definitions	136
10.1.2 What NAT Does	137
10.1.3 How NAT Works	137
10.1.4 NAT Application	138
10.1.5 NAT Mapping Types	139
10.2 Using NAT	140
10.2.1 SUA (Single User Account) Versus NAT	140
10.3 SUA Server	140
10.3.1 Default Server IP Address	141
10.3.2 Port Forwarding: Services and Port Numbers	141
10.3.3 Configuring Servers Behind SUA (Example)	142
10.4 Configuring SUA Server	143
10.5 Configuring Address Mapping	145
10.5.1 Configuring Address Mapping	147
10.6 Trigger Port Forwarding	148
10.6.1 Trigger Port Forwarding Example	148
10.6.2 Two Points To Remember About Trigger Ports	149
10.7 Configuring Trigger Port Forwarding	149

Chapter 11

Static Route Screens 152

11.1 Static Route Overview	152
11.2 Configuring IP Static Route	152
11.2.1 Configuring Route Entry	153

Chapter 12

Remote Management Screens 156

12.1 Remote Management Overview	156
12.1.1 Remote Management Limitations	156
12.1.2 Remote Management and NAT	157
12.1.3 System Timeout	157
12.2 Configuring WWW	157

12.3 Configuring Telnet	158
12.4 Configuring TELNET	159
12.5 Configuring FTP	160
12.6 SNMP	161
12.6.1 Supported MIBs	162
12.6.2 SNMP Traps	162
12.6.3 Configuring SNMP	163
12.7 Configuring DNS	165
12.8 Configuring Security	166
 Chapter 13	
UPnP.....	168
13.1 Universal Plug and Play Overview	168
13.1.1 How Do I Know If I'm Using UPnP?	168
13.1.2 NAT Traversal	168
13.1.3 Cautions with UPnP	168
13.2 UPnP and ZyXEL	169
13.3 Configuring UPnP	169
13.4 Installing UPnP in Windows Example	170
13.4.1 Installing UPnP in Windows Me	171
13.4.2 Installing UPnP in Windows XP	172
13.5 Using UPnP in Windows XP Example	173
13.5.1 Auto-discover Your UPnP-enabled Network Device	174
13.5.2 Web Configurator Easy Access	175
13.5.3 Web Configurator Easy Access	176
 Chapter 14	
Firewalls.....	178
14.1 Firewall Overview	178
14.2 Types of Firewalls	178
14.2.1 Packet Filtering Firewalls	178
14.2.2 Application-level Firewalls	178
14.2.3 Stateful Inspection Firewalls	179
14.3 Introduction to ZyXEL's Firewall	179
14.4 Denial of Service	180
14.4.1 Basics	180
14.4.2 Types of DoS Attacks	181
14.4.2.1 ICMP Vulnerability	184
14.4.2.2 Traceroute	184
14.5 Stateful Inspection	185
14.5.1 Stateful Inspection Process	185
14.5.2 Stateful Inspection and the ZyAIR	186
14.5.3 TCP Security	187

14.5.4 UDP/ICMP Security	187
14.5.5 Upper Layer Protocols	188
14.6 Guidelines For Enhancing Security With Your Firewall	188
14.7 Packet Filtering Vs Firewall	188
14.7.1 Packet Filtering:	189
14.7.1.1 When To Use Filtering	189
14.7.2 Firewall	189
14.7.2.1 When To Use The Firewall	189
Chapter 15	
Firewall Screens	192
15.1 Access Methods	192
15.2 Firewall Policies Overview	192
15.3 Rule Logic Overview	193
15.3.1 Rule Checklist	193
15.3.2 Security Ramifications	194
15.3.3 Key Fields For Configuring Rules	194
15.3.3.1 Action	194
15.3.3.2 Service	194
15.3.3.3 Source Address	194
15.3.3.4 Destination Address	194
15.4 Connection Direction Examples	195
15.4.1 LAN to WAN Rules	195
15.4.2 WAN to LAN Rules	195
15.5 Alerts	196
15.6 Configuring Firewall	196
15.6.1 Rule Summary	197
15.6.2 Configuring Firewall Rules	199
15.6.3 Configuring Custom Services	202
15.7 Example Firewall Rule	203
15.8 Predefined Services	206
Chapter 16	
Content Filtering	210
16.1 Introduction to Content Filtering	210
16.2 Restrict Web Features	210
16.3 Days and Times	210
16.4 Configure Content Filtering	210
Chapter 17	
Certificates	214
17.1 Certificates Overview	214
17.1.1 Advantages of Certificates	215

17.2 Self-signed Certificates	215
17.3 Configuration Summary	215
17.4 My Certificates	215
17.5 Certificate File Formats	218
17.6 Importing a Certificate	218
17.7 Creating a Certificate	219
17.8 My Certificate Details	222
17.9 Trusted CAs	225
17.10 Importing a Trusted CA's Certificate	227
17.11 Trusted CA Certificate Details	228
 Chapter 18	
Log Screens.....	232
18.1 Configuring View Log	232
18.2 Configuring Log Settings	233
18.3 Configuring Reports	236
 Chapter 19	
Maintenance	240
19.1 Maintenance Overview	240
19.2 System Status Screen	240
19.2.1 System Statistics	242
19.3 DHCP Table Screen	242
19.4 Association List	243
19.5 F/W Upload Screen	244
19.6 Configuration Screen	247
19.6.1 Backup Configuration	248
19.6.2 Restore Configuration	248
19.6.3 Back to Factory Defaults	250
19.7 Restart Screen	250
 Chapter 20	
Introducing the SMT	252
20.1 SMT Introduction	252
20.2 Connect to your ZyAIR Using Telnet	252
20.2.1 Entering Password	252
20.3 Changing the System Password	253
20.4 ZyAIR SMT Menu Overview Example	253
20.5 Navigating the SMT Interface	254
20.5.1 System Management Terminal Interface Summary	256
20.6 Changing the System Password	256

Chapter 21	
General Setup	258
21.1 General Setup	258
21.1.1 Procedure To Configure Menu 1	258
21.1.2 Procedure to Configure Dynamic DNS	260
Chapter 22	
Menu 2 WAN Setup	262
22.1 Introduction to WAN	262
22.2 WAN Setup	262
Chapter 23	
LAN Setup	264
23.1 LAN Setup	264
23.1.1 General Ethernet Setup	264
23.2 Protocol Dependent Ethernet Setup	265
23.3 TCP/IP Ethernet Setup and DHCP	265
23.3.1 IP Alias Setup	267
23.4 Wireless LAN Setup	268
23.4.1 Configuring MAC Address Filter	270
Chapter 24	
Internet Access	274
24.1 Introduction to Internet Access Setup	274
24.2 Ethernet Encapsulation	274
24.3 Configuring the PPTP Client	276
24.4 Configuring the PPPoE Client	277
24.5 Basic Setup Complete	278
Chapter 25	
Remote Node Configuration	280
25.1 Introduction to Remote Node Setup	280
25.2 Remote Node Profile Setup	280
25.2.1 Ethernet Encapsulation	280
25.2.2 PPPoE Encapsulation	282
25.2.2.1 Outgoing Authentication Protocol	283
25.2.2.2 Nailed-Up Connection	283
25.2.3 PPTP Encapsulation	284
25.3 Edit IP	285
25.4 Remote Node Filter	287

Chapter 26	
Static Route Setup	290
26.1 IP Static Route Setup	290
Chapter 27	
Dial-in User Setup	292
27.1 Dial-in User Setup	292
Chapter 28	
Network Address Translation (NAT)	294
28.1 Using NAT	294
28.1.1 SUA (Single User Account) Versus NAT	294
28.2 Applying NAT	294
28.3 NAT Setup	296
28.3.1 Address Mapping Sets	297
28.3.1.1 User-Defined Address Mapping Sets	298
28.3.1.2 Ordering Your Rules	299
28.4 Configuring a Server behind NAT	301
28.5 General NAT Examples	302
28.5.1 Example 1: Internet Access Only	302
28.5.2 Example 2: Internet Access with an Inside Server	303
28.5.3 Example 3: Multiple Public IP Addresses With Inside Servers	304
28.5.4 Example 4: NAT Unfriendly Application Programs	308
28.6 Configuring Trigger Port Forwarding	310
Chapter 29	
Filter Configuration	312
29.1 Introduction to Filters	312
29.1.1 The Filter Structure of the ZyAIR	313
29.2 Configuring a Filter Set	314
29.2.1 Configuring a Filter Rule	316
29.2.2 Configuring a TCP/IP Filter Rule	317
29.2.3 Configuring a Generic Filter Rule	319
29.3 Example Filter	321
29.4 Filter Types and NAT	323
29.5 Firewall Versus Filters	324
29.6 Applying a Filter	324
29.6.1 Applying LAN Filters	324
29.6.2 Applying Remote Node Filters	325
Chapter 30	
Enabling the Firewall	326
30.1 Remote Management and the Firewall	326

30.2 Access Methods	326
30.3 Enabling the Firewall	326
Chapter 31	
SNMP Configuration	328
31.1 About SNMP	328
31.2 Supported MIBs	329
31.3 SNMP Configuration	329
31.4 SNMP Traps	330
Chapter 32	
System Security	332
32.1 System Security	332
32.1.1 System Password	332
32.1.2 Configuring External RADIUS Server	332
32.1.3 802.1x	334
Chapter 33	
System Information and Diagnosis	338
33.1 System Status	338
33.2 System Information	340
33.2.1 System Information	340
33.2.2 Console Port Speed	341
33.3 Log and Trace	341
33.3.1 Viewing Error Log	341
33.3.2 UNIX Syslog	342
33.3.2.1 CDR	343
33.3.2.2 Packet triggered	343
33.3.2.3 Filter log	344
33.3.2.4 PPP log	344
33.3.2.5 Firewall log	345
33.3.3 Call-Triggering Packet	345
33.4 Diagnostic	346
33.4.1 WAN DHCP	347
Chapter 34	
Firmware and Configuration File Maintenance	350
34.1 Filename Conventions	350
34.2 Backup Configuration	351
34.2.1 Backup Configuration Using FTP	351
34.2.2 Using the FTP command from the DOS Prompt	352
34.2.3 GUI-based FTP Clients	353
34.2.4 TFTP and FTP over WAN Management Limitations	353

34.2.5 Backup Configuration Using TFTP	354
34.2.6 Example: TFTP Command	354
34.2.7 GUI-based TFTP Clients	355
34.3 Restore Configuration	355
34.3.1 Restore Using FTP	355
34.3.2 Restore Using FTP Session Example	356
34.4 Uploading Firmware and Configuration Files	357
34.4.1 Firmware Upload	357
34.4.2 Configuration File Upload	358
34.4.3 Using the FTP command from the DOS Prompt Example	358
34.4.4 TFTP File Upload	359
34.4.5 Example: TFTP Command	360
Chapter 35	
System Maintenance and Information	362
35.1 Command Interpreter Mode	362
35.2 Call Control Support	363
35.2.1 Budget Management	364
35.2.2 Call History	364
35.3 Time and Date Setting	365
35.3.1 Resetting the Time	367
Chapter 36	
Remote Management	368
36.1 Remote Management	368
36.1.1 Telnet	369
36.1.2 FTP	370
36.1.3 Web	370
36.1.4 Remote Management Limitations	370
36.2 Remote Management and NAT	370
36.3 System Timeout	371
Chapter 37	
Call Scheduling	372
37.1 Introduction to Call Scheduling	372
Appendix A	
Troubleshooting	376
Appendix B	
Brute-Force Password Guessing Protection	378
Appendix C	
Setting up Your Computer's IP Address	380

Appendix D	
IP Address Assignment Conflicts	392
 Appendix E	
IP Subnetting	396
 Appendix F	
Command Interpreter.....	404
 Appendix G	
Log Descriptions	406
 Appendix H	
Wireless LAN and IEEE 802.11	410
 Appendix I	
Wireless LAN With IEEE 802.1x	414
 Appendix J	
Types of EAP Authentication	418
 Appendix K	
Antenna Selection and Positioning Recommendation.....	420
 Appendix L	
Power Adaptor Specifications	422

List of Figures

Figure 1 Internet Access Application Example	42
Figure 2 Change Password Screen	45
Figure 3 Replace Certificate Screen	45
Figure 4 The MAIN MENU Screen of the Web Configurator	47
Figure 5 Wizard 1 : General Setup	50
Figure 6 Wizard 2 : Wireless LAN Setup	51
Figure 7 Wizard 3: Wireless LAN Setup: Basic Security	52
Figure 8 Wizard 3: Wireless LAN Setup: Extend Security	53
Figure 9 Wizard 4: Ethernet Encapsulation	54
Figure 10 Wizard 4: PPPoE Encapsulation	56
Figure 11 Wizard 4: PPTP Encapsulation	57
Figure 12 Wizard 5: WAN Setup	61
Figure 13 Wizard Finish	63
Figure 14 System General Setup	64
Figure 15 DDNS	66
Figure 16 Password.	67
Figure 17 Time Setting	68
Figure 18 LAN IP	73
Figure 19 Static DHCP	76
Figure 20 IP Alias	77
Figure 21 IBSS (Ad-hoc) Wireless LAN	78
Figure 22 Basic Service set	79
Figure 23 Extended Service Set	80
Figure 24 RTS/CTS	81
Figure 25 Wireless	83
Figure 26 Roaming Example	84
Figure 27 Roaming	86
Figure 28 ZyAIR Wireless Security Levels	88
Figure 29 Wireless: No Security	89
Figure 30 WEP Authentication Steps	91
Figure 31 Wireless: Static WEP Encryption	92
Figure 32 WPA - PSK Authentication	95
Figure 33 Wireless: WPA-PSK	96
Figure 34 WPA with RADIUS Application Example	98
Figure 35 Wireless: WPA	99
Figure 36 EAP Authentication	101

Figure 37 Wireless: WPA	103
Figure 38 Wireless: 802.1x and Dynamic WEP	106
Figure 39 Wireless: 802.1x and Static WEP	108
Figure 40 Wireless: 802.1x	111
Figure 41 MAC Address Filter	113
Figure 42 ZyAIR Authenticates Wireless Stations	115
Figure 43 ZyAIR Authenticates other AP's	115
Figure 44 Internal RADIUS Server Setting Screen	117
Figure 45 Trusted AP Overview	118
Figure 46 Trusted AP Screen	119
Figure 47 Trusted Users Screen	121
Figure 48 Ethernet Encapsulation	125
Figure 49 Ethernet Encapsulation	126
Figure 50 PPPoE Encapsulation	128
Figure 51 PPTP Encapsulation	130
Figure 52 WAN: IP	132
Figure 53 MAC Setup	134
Figure 54 How NAT Works	138
Figure 55 NAT Application With IP Alias	139
Figure 56 Multiple Servers Behind NAT Example	143
Figure 57 SUA/NAT Setup	144
Figure 58 Address Mapping	146
Figure 59 Address Mapping Edit	147
Figure 60 Trigger Port Forwarding Process: Example	149
Figure 61 Trigger Port	150
Figure 62 Example of Static Routing Topology	152
Figure 63 Static Route	153
Figure 64 Static Route: Edit	154
Figure 65 Remote Management: WWW	158
Figure 66 Telnet Configuration on a TCP/IP Network	159
Figure 67 Remote Management: Telnet	159
Figure 68 Remote Management: FTP	160
Figure 69 SNMP Management Model	161
Figure 70 Remote Management: SNMP	164
Figure 71 Remote Management: DNS	165
Figure 72 Security	167
Figure 73 Configuring UPnP	170
Figure 74 ZyAIR Firewall Application	180
Figure 75 Three-Way Handshake	182
Figure 76 SYN Flood	183
Figure 77 Smurf Attack	184
Figure 78 Stateful Inspection	185
Figure 79 LAN to WAN Traffic	195

Figure 80 WAN to LAN Traffic	196
Figure 81 Default Rule	197
Figure 82 Rule Summary	198
Figure 83 Creating/Editing A Firewall Rule	200
Figure 84 Creating/Editing A Custom Service	202
Figure 85 Rule Summary	203
Figure 86 Rule Edit Example	204
Figure 87 Edit Custom Service Example	204
Figure 88 My Service Rule Configuration	205
Figure 89 My Service Example Rule Summary	206
Figure 90 Content Filter	211
Figure 91 My Certificates	216
Figure 92 My Certificate Import	219
Figure 93 My Certificate Create	220
Figure 94 My Certificate Details	223
Figure 95 Trusted CAs	226
Figure 96 Trusted CA Import	227
Figure 97 Trusted CA Details	229
Figure 98 View Log	232
Figure 99 Log Settings	234
Figure 100 Reports	237
Figure 101 System Status	241
Figure 102 System Status: Show Statistics	242
Figure 103 Maintenance DHCP Table	243
Figure 104 Association List	244
Figure 105 Firmware Upload	245
Figure 106 Firmware Upload In Process	246
Figure 107 Network Temporarily Disconnect	246
Figure 108 Firmware Upload Error	247
Figure 109 Configuration	248
Figure 110 Configuration Upload Successful	249
Figure 111 Network Temporarily Disconnected	249
Figure 112 Configuration Upload Error	250
Figure 113 Reset Warning Message	250
Figure 114 Restart Screen	251
Figure 115 Login Screen	252
Figure 116 Login Screen	253
Figure 117 Menu 23.1 System Security : Change Password	253
Figure 118 ZyAIR G-2000 Plus SMT Menu Overview Example	254
Figure 119 ZyAIR G-2000 Plus SMT Main Menu	256
Figure 120 Menu 23: System Security	257
Figure 121 Menu 23 System Password	257
Figure 122 Menu 1 General Setup	259

Figure 123 Menu 1.1 Configure Dynamic DNS	260
Figure 124 Menu 2 WAN Setup	262
Figure 125 Menu 3 LAN Setup	264
Figure 126 Menu 3.1 LAN Port Filter Setup.	264
Figure 127 Menu 3.2 TCP/IP Setup	265
Figure 128 Physical Network & Partitioned Logical Networks	267
Figure 129 Menu 3.2.1: IP Alias Setup	268
Figure 130 Menu 3.5 Wireless LAN Setup	269
Figure 131 Menu 3.5 Wireless LAN Setup	271
Figure 132 Menu 3.5.1 WLAN MAC Address Filter	272
Figure 133 Menu 4 Internet Access Setup	275
Figure 134 Internet Access Setup (PPTP)	277
Figure 135 Internet Access Setup (PPPoE)	278
Figure 136 Menu 11.1 Remote Node Profile for Ethernet Encapsulation	281
Figure 137 Menu 11.1 Remote Node Profile for PPPoE Encapsulation	283
Figure 138 Menu 11.1 Remote Node Profile for PPTP Encapsulation	285
Figure 139 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation .	286
Figure 140 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)	288
Figure 141 Menu 11.5: Remote Node Filter (PPPoE and PPTP Encapsulation)	288
Figure 142 Menu 12 IP Static Route Setup	290
Figure 143 Menu12.1 Edit IP Static Route	291
Figure 144 Menu 14- Dial-in User Setup	292
Figure 145 Menu 14.1- Edit Dial-in User	293
Figure 146 Menu 4 Applying NAT for Internet Access	295
Figure 147 Menu 11.3 Applying NAT to the Remote Node	296
Figure 148 Menu 15 NAT Setup	297
Figure 149 Menu 15.1 Address Mapping Sets	297
Figure 150 Menu 15.1.255 SUA Address Mapping Rules	298
Figure 151 Menu 15.1.1 First Set	299
Figure 152 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set	300
Figure 153 Menu 15.2.1 NAT Server Setup	301
Figure 154 Multiple Servers Behind NAT Example	302
Figure 155 NAT Example 1	303
Figure 156 Menu 4 Internet Access & NAT Example	303
Figure 157 NAT Example 2	304
Figure 158 Menu 15.2.1 Specifying an Inside Server	304
Figure 159 NAT Example 3	305
Figure 160 NAT Example 3: Menu 11.3	306
Figure 161 Example 3: Menu 15.1.1.1	307
Figure 162 Example 3: Final Menu 15.1.1	307
Figure 163 Example 3: Menu 15.2	308
Figure 164 NAT Example 4	309
Figure 165 Example 4: Menu 15.1.1.1 Address Mapping Rule.	309

Figure 166 Example 4: Menu 15.1.1 Address Mapping Rules	310
Figure 167 Menu 15.3 Trigger Port Setup	311
Figure 168 Outgoing Packet Filtering Process	312
Figure 169 Filter Rule Process	314
Figure 170 Menu 21: Filter and Firewall Setup	315
Figure 171 Menu 21.1: Filter Set Configuration	315
Figure 172 Menu 21.1.1.1 TCP/IP Filter Rule.	317
Figure 173 Executing an IP Filter	319
Figure 174 Menu 21.1.4.1 Generic Filter Rule	320
Figure 175 Telnet Filter Example	321
Figure 176 Example Filter: Menu 21.1.3.1	322
Figure 177 Example Filter Rules Summary: Menu 21.1.3	323
Figure 178 Protocol and Device Filter Sets	324
Figure 179 Filtering LAN Traffic	325
Figure 180 Filtering Remote Node Traffic	325
Figure 181 Menu 21.2 Firewall Setup	327
Figure 182 SNMP Management Model	328
Figure 183 Menu 22 SNMP Configuration	330
Figure 184 Menu 23 System Security	332
Figure 185 Menu 23 System Security	333
Figure 186 Menu 23.2 System Security : RADIUS Server	333
Figure 187 Menu 23 System Security	334
Figure 188 Menu 23.4 System Security : IEEE802.1x	335
Figure 189 Menu 24 System Maintenance	338
Figure 190 Menu 24.1 System Maintenance : Status	339
Figure 191 Menu 24.2 System Information and Console Port Speed	340
Figure 192 Menu 24.2.1 System Information : Information	340
Figure 193 Menu 24.2.2 System Maintenance : Change Console Port Speed	341
Figure 194 Menu 24.3 System Maintenance : Log and Trace	342
Figure 195 Menu 24.3.2 System Maintenance : UNIX Syslog	342
Figure 196 Call-Triggering Packet Example	346
Figure 197 LAN & WAN DHCP	347
Figure 198 Menu 24.5 Backup Configuration	352
Figure 199 FTP Session Example	353
Figure 200 Menu 24.6 Restore Configuration	356
Figure 201 Restore Using FTP Session Examplei	356
Figure 202 Menu 24.7 System Maintenance: Upload Firmware	357
Figure 203 Menu 24.7.1 System Maintenance : Upload System Firmware	358
Figure 204 Menu 24.7.2 System Maintenance: Upload System Configuration File	358
Figure 205 FTP Session Example	359
Figure 206 Menu 24 System Maintenance	363
Figure 207 Valid CI Commands	363
Figure 208 Menu 24.9 System Maintenance : Call Control	364

Figure 209 Budget Management	364
Figure 210 Menu 24.9.2 - Call History	365
Figure 211 Menu 24.10 System Maintenance : Time and Date Setting	366
Figure 212 Menu 24.11 – Remote Management Control	369
Figure 213 Telnet Configuration on a TCP/IP Network	370
Figure 214 Menu 26 Schedule Setup	372
Figure 215 Menu 26.1 Schedule Set Setup	373
Figure 216 Applying Schedule Set(s) to a Remote Node (PPPoE)	374
Figure 217 WIndows 95/98/Me: Network: Configuration	381
Figure 218 Windows 95/98/Me: TCP/IP Properties: IP Address	382
Figure 219 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	383
Figure 220 Windows XP: Start Menu	384
Figure 221 Windows XP: Control Panel	384
Figure 222 Windows XP: Control Panel: Network Connections: Properties	385
Figure 223 Windows XP: Local Area Connection Properties	385
Figure 224 Windows XP: Advanced TCP/IP Settings	386
Figure 225 Windows XP: Internet Protocol (TCP/IP) Properties	387
Figure 226 Macintosh OS 8/9: Apple Menu	388
Figure 227 Macintosh OS 8/9: TCP/IP	388
Figure 228 Macintosh OS X: Apple Menu	389
Figure 229 Macintosh OS X: Network	390
Figure 230 IP Address Conflicts: CaseA	392
Figure 231 IP Address Conflicts: Case B	393
Figure 232 IP Address Conflicts: Case C	393
Figure 233 IP Address Conflicts: Case D	394
Figure 234 Peer-to-Peer Communication in an Ad-hoc Network	411
Figure 235 ESS Provides Campus-Wide Coverage	412
Figure 236 Sequences for EAP MD5–Challenge Authentication	415
Figure 237 Sequences for PEAP, MS–CHAP V2 Authentication	416

List of Tables

Table 1 IEEE 802.11b	37
Table 2 IEEE 802.11g	38
Table 3 Wizard 1 : General Setup	50
Table 4 Wizard 2 : Wireless LAN Setup	51
Table 5 Wizard 3: Wireless LAN Setup: Basic Security	52
Table 6 Wizard 3: Wireless LAN Setup: Extend Security	53
Table 7 Wizard 4: Ethernet Encapsulation	54
Table 8 Wizard 4: PPPoE Encapsulation	56
Table 9 Wizard 4: PPTP Encapsulation	57
Table 10 Private IP Address Ranges	58
Table 11 Example of Network Properties for LAN Servers with Fixed IP Addresses	60
Table 12 Wizard 5: WAN Setup	61
Table 13 System General Setup	64
Table 14 DDNS	66
Table 15 Password	67
Table 16 Time Setting	68
Table 17 LAN IP	73
Table 18 Static DHCP	76
Table 19 IP Alias	77
Table 20 Wireless	83
Table 21 Roaming	86
Table 22 Wireless No Security	89
Table 23 Wireless Security Relational Matrix	90
Table 24 Wireless: Static WEP Encryption	92
Table 25 Wireless: WPA-PSK	96
Table 26 Wireless: WPA	99
Table 27 RADIUS	103
Table 28 Wireless: 802.1x and Dynamic WEP	106
Table 29 Wireless: 802.1x and Static WEP	108
Table 30 Wireless: 802.1x and No WEP	111
Table 31 MAC Address Filter	113
Table 32 Internal RADIUS Server	115
Table 33 My Certificates	117
Table 34 Trusted AP	119
Table 35 Trusted Users	121
Table 36 Ethernet Encapsulation	125

Table 37 Ethernet Encapsulation	126
Table 38 PPPoE Encapsulation	128
Table 39 PPTP Encapsulation	130
Table 40 WAN: IP	132
Table 41 NAT Definitions	136
Table 42 NAT Mapping Types	140
Table 43 Services and Port Numbers	142
Table 44 SUA/NAT Setup	144
Table 45 Address Mapping	146
Table 46 Address Mapping Edit	147
Table 47 Trigger Port	150
Table 48 Static Route	153
Table 49 Static Route: Edit	154
Table 50 Remote Management: WWW	158
Table 51 Remote Management: Telnet	159
Table 52 Remote Management: FTP	160
Table 53 SNMP Traps	162
Table 54 Remote Management: SNMP	164
Table 55 Remote Management: DNS	165
Table 56 Security	167
Table 57 Configuring UPnP	170
Table 58 Common IP Ports	180
Table 59 ICMP Commands That Trigger Alerts	184
Table 60 Default Rule	197
Table 61 Rule Summary	198
Table 62 Creating/Editing A Firewall Rule	201
Table 63 Creating/Editing A Custom Service	202
Table 64 Predefined Services	206
Table 65 Content Filter	211
Table 66 My Certificates	216
Table 67 My Certificate Import	219
Table 68 My Certificate Create	221
Table 69 My Certificate Details	224
Table 70 Trusted CAs	226
Table 71 Trusted CA Import	227
Table 72 Trusted CA Details	230
Table 73 View Log	232
Table 74 Log Settings	235
Table 75 Reports	237
Table 76 System Status	241
Table 77 System Status: Show Statistics	242
Table 78 Maintenance DHCP Table	243
Table 79 Association List	244

Table 80 Firmware Upload	245
Table 81 Restore Configuration	248
Table 82 Main Menu Commands	254
Table 83 Main Menu Summary	256
Table 84 Menu 1 General Setup	259
Table 85 Menu 1.1 Configure Dynamic DNS	260
Table 86 Menu 2 WAN Setup	262
Table 87 DHCP Ethernet Setup Fields	265
Table 88 Menu 3.2: LAN TCP/IP Setup Fields	266
Table 89 Menu 3.2.1: IP Alias Setup	268
Table 90 Menu 3.5 Wireless LAN Setup	269
Table 91 Menu 3.5.1 WLAN MAC Address Filter	272
Table 92 Internet Access Setup (Ethernet)	275
Table 93 New Fields in Menu 4 (PPTP) Screen	277
Table 94 New Fields in Menu 4 (PPPoE) screen	278
Table 95 Menu 11.1 Remote Node Profile for Ethernet Encapsulation	281
Table 96 Fields in Menu 11.1 (PPPoE Encapsulation Specific)	284
Table 97 Menu 11.1 Remote Node Profile for PPTP Encapsulation	285
Table 98 Remote Node Network Layer Options	286
Table 99 Menu 12.1 Edit IP Static Route	291
Table 100 Menu 14.1- Edit Dial-in User	293
Table 101 Applying NAT in Menus 4 & 11.3	296
Table 102 SUA Address Mapping Rules	298
Table 103 Menu 15.1.1 First Set	299
Table 104 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set	300
Table 105 Menu 15.3 Trigger Port Setup	311
Table 106 Abbreviations Used in the Filter Rules Summary Menu	315
Table 107 Rule Abbreviations Used	316
Table 108 TCP/IP Filter Rule	317
Table 109 Generic Filter Rule Menu Fields	320
Table 110 Menu 22 SNMP Configuration	330
Table 111 SNMP Traps	330
Table 112 Ports and Interface Types	331
Table 113 Menu 23.2 System Security : RADIUS Server	333
Table 114 Menu 23.4 System Security : IEEE802.1x	335
Table 115 Menu 24.1 System Maintenance : Status	339
Table 116 Menu 24.2.1 System Maintenance : Information	340
Table 117 Menu 24.3.2 System Maintenance : UNIX Syslog	342
Table 118 Menu 24.4 System Maintenance Menu: Diagnostic	347
Table 119 Filename Conventions	351
Table 120 General Commands for Third Party FTP Clients	353
Table 121 General Commands for Third Party TFTP Clients	355
Table 122 Menu 24.9.1 - Budget Management	364

Table 123 Call History Fields	365
Table 124 System Maintenance : Time and Date Setting	366
Table 125 Menu 24.11 – Remote Management Control	369
Table 126 Menu 26.1 Schedule Set Setup	373
Table 127 Troubleshooting the Start-Up of Your ZyAIR	376
Table 128 Troubleshooting the Ethernet Interface	376
Table 129 Troubleshooting the Password	377
Table 130 Troubleshooting Telnet	377
Table 131 Troubleshooting the WLAN Interface	377
Table 132 Brute-Force Password Guessing Protection Commands	378
Table 133 Classes of IP Addresses	396
Table 134 Allowed IP Address Range By Class	397
Table 135 “Natural” Masks	397
Table 136 Alternative Subnet Mask Notation	398
Table 137 Two Subnets Example	398
Table 138 Subnet 1	399
Table 139 Subnet 2	399
Table 140 Subnet 1	400
Table 141 Subnet 2	400
Table 142 Subnet 3	400
Table 143 Subnet 4	401
Table 144 Eight Subnets	401
Table 145 Class C Subnet Planning	401
Table 146 Class B Subnet Planning	402
Table 147 System Error Logs	406
Table 148 System Maintenance Logs	406
Table 149 ICMP Notes	406
Table 150 Sys log	407
Table 151 Log Categories and Available Settings	408
Table 152 Comparison of EAP Authentication Types	419
Table 153 NORTH AMERICAN PLUG STANDARDS	422
Table 154 NORTH AMERICAN PLUG STANDARDS	422
Table 155 EUROPEAN PLUG STANDARDS	422
Table 156 United Kingdom PLUG STANDARDS	422
Table 157 Japan PLUG STANDARDS	422
Table 158 Australia and New Zealand plug standards	423

Preface

Congratulations on your purchase of the ZyAIR G-2000 Plus - 802.11g Wireless 4 port Router.

A wireless router is an access point and router rolled into one. It is a cost-effect solution to share Internet access with multiple computers and expand your wired network.

Your ZyAIR is easy to install and configure.



Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

About This User's Guide

This User's Guide is designed to guide you through the configuration of your ZyAIR using the web configurator or the SMT. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator



Note: Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your ZyAIR. Not all features can be configured through all interfaces.

Related Documentation

- Supporting Disk

Refer to the included CD for support documents.

- Compact Guide

The Quick Start Guide is designed to help you get up and running right away. It contains connection information and instructions on getting started.

- Web Configurator Online Help

Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site

Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.











User Guide Feedback

Help us help you! E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The ZyAIR G-2000 Plus may be referred to simply as the ZyAIR in the user’s guide.

Graphics Icons Key

ZyAIR 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Modem 	Switch 	Router 
Wireless Signal 		

CHAPTER 1

Getting to Know Your ZyAIR

This chapter introduces the main features and applications of the ZyAIR.

1.1 Introducing the ZyAIR

The ZyAIR G-2000 Plus, an IEEE802.11g compliant broadband wireless sharing gateway, provides wireless connectivity. As an Internet gateway, your ZyAIR can share an Internet connection (through a cable or xDSL modem) with multiple computers using SUA/NAT and DHCP. The ZyAIR offers highly secured wireless connectivity to your wired network with IEEE 802.1X, WEP data encryption, WPA (Wi-Fi Protected Access) and MAC address filtering.

The ZyAIR is easy to install and configure. The embedded web-based configurator and SNMP network management enables remote configuration and management of your ZyAIR.

1.2 ZyAIR Features

The following sections describe the features of the ZyAIR

1.2.1 Physical Features

1.2.1.1 4-Port Switch

A combination of switch and router makes your ZyAIR a cost-effective and viable network solution. You can connect up to four computers to the LAN ports on your ZyAIR without the cost of a hub.

1.2.1.2 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface

This auto-negotiating feature allows the ZyAIR to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

1.2.1.3 10/100M Auto-crossover Ethernet/Fast Ethernet Interface

The LAN interface automatically adjusts to either a crossover or straight-through Ethernet cable.

1.2.1.4 10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router.

1.2.1.5 Reset Button

The ZyAIR reset button is built into the side panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33. .

1.2.1.6 ZyAIR LED

The blue ZyAIR LED (also known as the Breathing LED) is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. You may use the web configurator to turn this LED off even when the ZyAIR is on and data is being transmitted/received.

1.2.2 Firmware Features

1.2.2.1 Internal RADIUS Server

The ZyAIR has a built-in RADIUS server that can authenticate wireless clients or other AP's in other wireless networks. The ZyAIR can also function as an AP and as a RADIUS server at the same time.

1.2.2.2 Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

1.2.2.3 802.11b Wireless LAN Standard

The ZyAIR complies with the 802.11b wireless standard.

The 802.11b data rate and corresponding modulation techniques are shown in the table below. The modulation technique defines how bits are encoded onto radio waves.

Table 1 IEEE 802.11b

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)

1.2.2.4 802.11g Wireless LAN Standard

The ZyAIR, complies with the 802.11g wireless standard and is also fully compatible with the 802.11b standard. This means an 802.11b radio card can interface directly with an 802.11g device (and vice versa) at 11 Mbps or lower depending on range. 802.11g has several intermediate rate steps between the maximum and minimum data rates. The 802.11g data rate and modulation are as follows:

Table 2 IEEE 802.11g

DATA RATE (Mbps)	MODULATION
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)



Note: The ZyAIR may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

1.2.2.5 STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network.

1.2.2.6 Certificates

The ZyAIR can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

1.2.2.7 Limit the number of Client Connections

You may set a maximum number of wireless stations that may connect to the ZyAIR. This may be necessary if for example, there is interference or difficulty with channel assignment due to a high density of APs within a coverage area.

1.2.2.8 SSL Passthrough

SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https" instead of "http". The ZyAIR allows SSL connections to take place through the ZyAIR.

1.2.2.9 Firewall

The ZyAIR employs a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyAIR firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

1.2.2.10 Brute-Force Password Guessing Protection

The ZyAIR has a special protection mechanism to discourage brute-force password guessing attacks on the ZyAIR's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendix for details about this feature.

1.2.2.11 Wireless LAN MAC Address Filtering

Your ZyAIR checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

1.2.2.12 WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

1.2.2.13 IEEE 802.1X Network Security

The ZyAIR supports the IEEE 802.1x standard to enhance user authentication. Use the built-in user profile database to authenticate up to 32 users using MD5 encryption. Use an EAP-compatible RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate a limitless number of users using EAP (Extensible Authentication Protocol). EAP is an authentication protocol that supports multiple types of authentication.

1.2.2.14 Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the ZyAIR and other UPnP-enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

1.2.2.15 Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service.

1.2.2.16 PPPoE Support (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the ZyAIR is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

1.2.2.17 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. Use PPTP to connect to a broadband modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

1.2.2.18 Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translations of multiple IP addresses used within one network to different IP addresses known within another network.

1.2.2.19 Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway on the LAN when the ZyAIR cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

1.2.2.20 NAT for Single-IP-address Internet Access

The ZyAIR's SUA (Single User Account) feature allows multiple-user Internet access for the cost of a single IP account. NAT supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealPlayer, VDOLive, Quake, and PPTP. No configuration is needed to support these applications.

1.2.2.21 DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyAIR has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The ZyAIR also acts as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

1.2.2.22 Multicast

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236). The ZyAIR supports versions 1 and 2.

1.2.2.23 IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The ZyAIR supports three logical LAN interfaces via its single physical Ethernet LAN interface with the ZyAIR itself as the gateway for each LAN network.

1.2.2.24 IP Policy Routing

IP Policy Routing provides a mechanism to override the default routing behavior and alter packet forwarding based on the policies defined by the network administrator.

1.2.2.25 SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

1.2.2.26 Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyAIR's management settings. Most functions of the ZyAIR are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection.

1.2.2.27 Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.

1.2.2.28 Diagnostics Capabilities

The ZyAIR can perform self-diagnostic tests. These tests check the integrity of the following circuitry:

- FLASH memory
- DRAM
- LAN port
- Wireless port

1.2.2.29 Embedded FTP and TFTP Servers

The ZyAIR's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

1.2.2.30 Wireless Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the ZyAIR to access your wired network.

1.2.2.31 Wireless LAN Channel Usage

The **Wireless Channel Usage** screen displays whether the radio channels are used by other wireless devices within the transmission range of the ZyAIR. This allows you to select the channel with minimum interference for your ZyAIR.

1.3 Applications for the ZyAIR

Here is an application example of what you can do with your ZyAIR.

1.3.1 Internet Access Application

Add a wireless LAN to your existing network without expensive network cables. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.

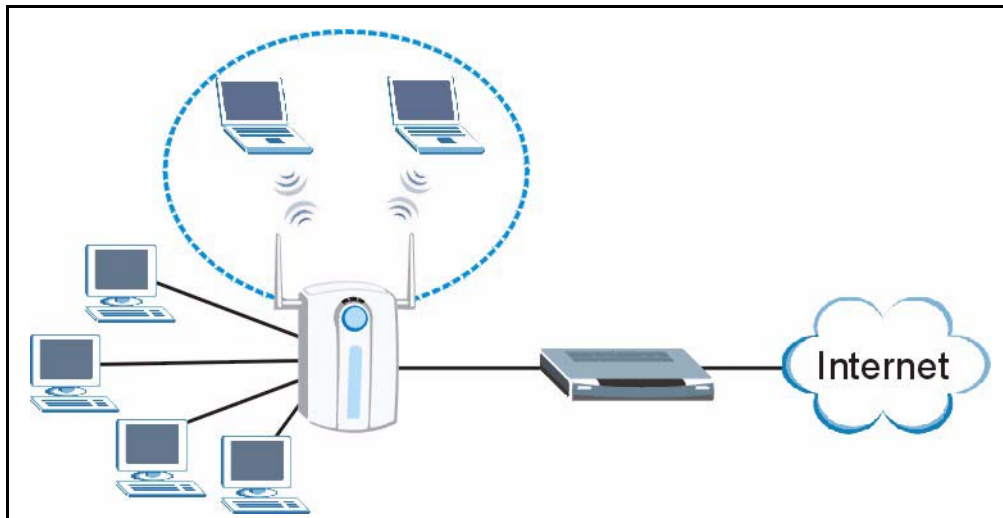


Figure 1 Internet Access Application Example

CHAPTER 2

Introducing the Web Configurator

This chapter describes how to access the ZyAIR web configurator and provides an overview of its screens. The default IP address of the ZyAIR is 192.168.1.1.

2.1 Web Configurator Overview

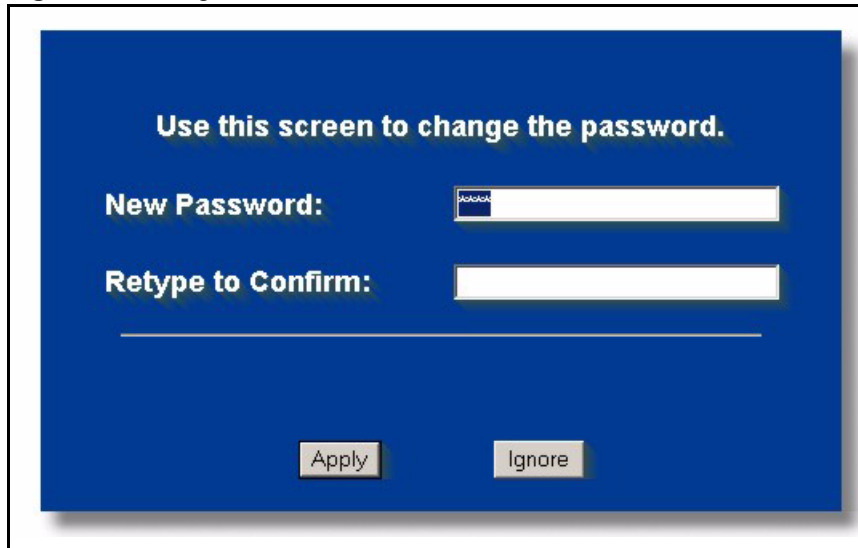
The embedded web configurator (ewc) allows you to manage the ZyAIR from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual firmware versions.

2.2 Accessing the ZyAIR Web Configurator

- 1 Make sure your ZyAIR hardware is properly connected and prepare your computer/ computer network to connect to the ZyAIR (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.



Note: If you do not change the password, the following screen appears every time you login.

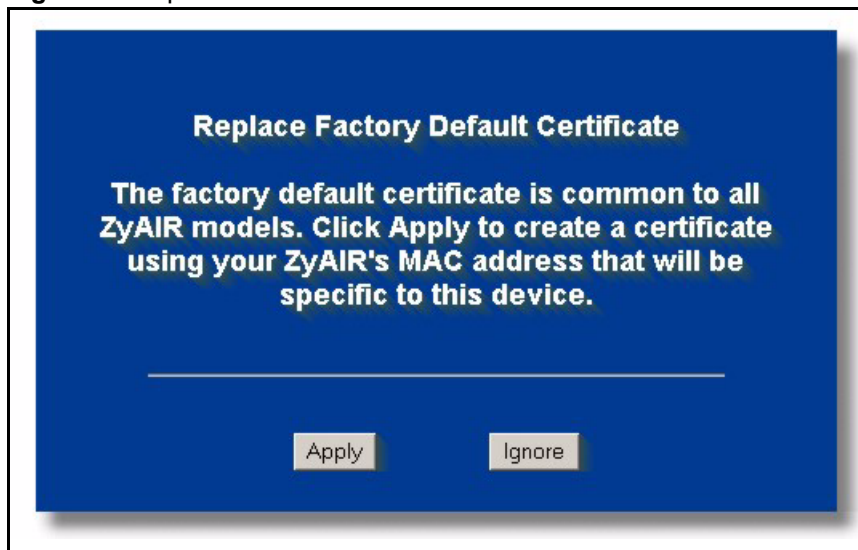
Figure 2 Change Password ScreenA screenshot of a web-based password change interface. The background is blue. At the top, white text reads "Use this screen to change the password." Below this, there are two white input fields. The first is labeled "New Password:" and has a small blue icon to its left. The second is labeled "Retype to Confirm:" and is empty. At the bottom, there are two buttons: "Apply" and "Ignore".

Use this screen to change the password.

New Password:

Retype to Confirm:

- 6** Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyAIR's MAC address that will be specific to this device.

Figure 3 Replace Certificate ScreenA screenshot of a web-based screen titled "Replace Factory Default Certificate". The background is blue. The title is in white. Below the title, white text reads: "The factory default certificate is common to all ZyAIR models. Click Apply to create a certificate using your ZyAIR's MAC address that will be specific to this device." At the bottom, there are two buttons: "Apply" and "Ignore".

Replace Factory Default Certificate

The factory default certificate is common to all ZyAIR models. Click Apply to create a certificate using your ZyAIR's MAC address that will be specific to this device.

You should now see the **MAIN MENU** screen..



Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the ZyAIR if this happens to you.

2.3 Resetting the ZyAIR

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the side panel of the ZyAIR. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to 1234, also.

2.3.1 Procedure To Use The Reset Button

Make sure the **SYS LED** is on (not blinking) before you begin this procedure.

- 1 Press the **RESET** button for ten seconds or until the **SYS LED**, **LINK LED** or **BRI/RPT LED** turns red, and then release it. If the **SYS LED** begins to blink, the defaults have been restored and the ZyAIR restarts. Otherwise, go to step 2.
- 2 Turn the ZyAIR off.
- 3 While pressing the **RESET** button, turn the ZyAIR on.
- 4 Continue to hold the **RESET** button. The **SYS LED** will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the ZyAIR is now restarting.
- 5 Release the **RESET** button and wait for the ZyAIR to finish restarting.


2.3.2 Method of Restoring Factory-Defaults Via Web Configurator

Use the web configurator to restore defaults (refer to the Maintenance chapter).

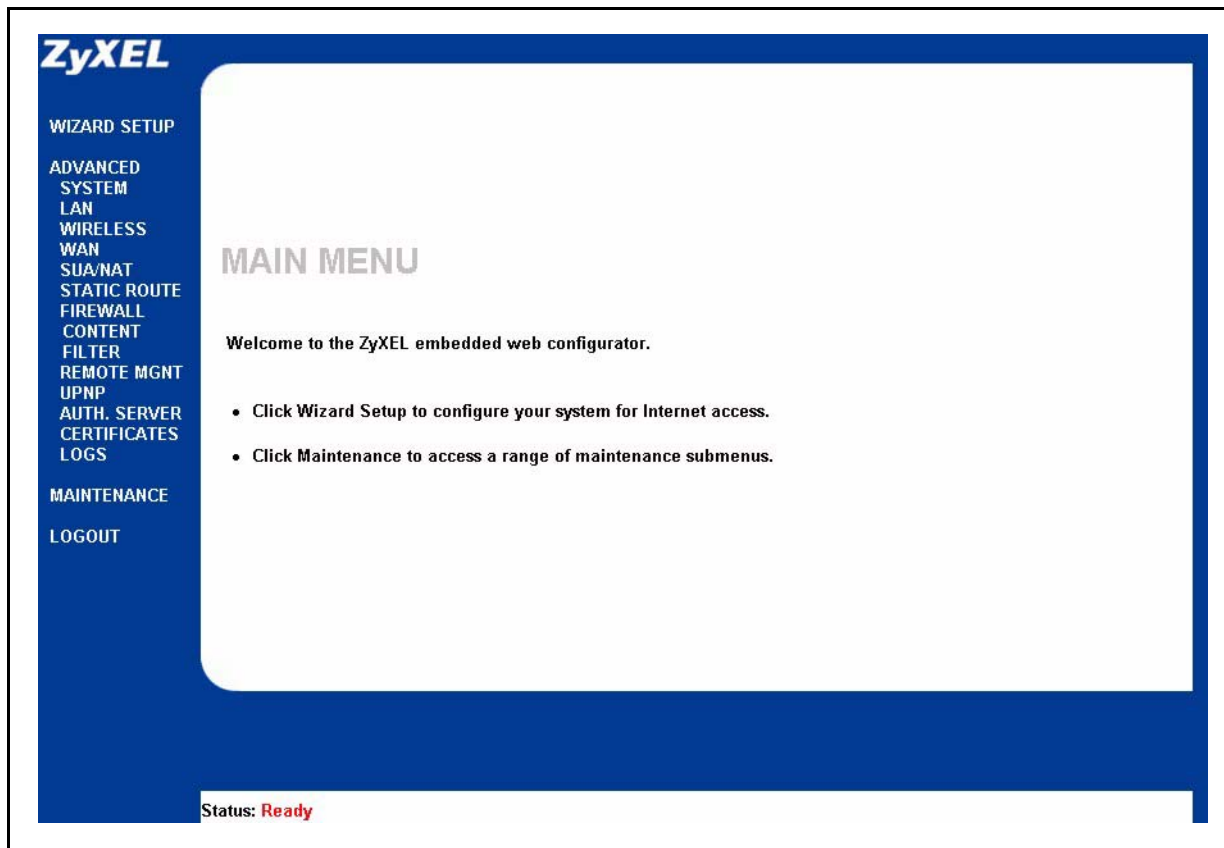
2.4 Navigating the ZyAIR Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.



Note: Follow the instructions you see in the **MAIN MENU** screen or click the  icon (located in the top right corner of most screens) to view online help.

The  icon does not appear in the **MAIN MENU** screen.

Figure 4 The MAIN MENU Screen of the Web Configurator

Use submenus to configure ZyAIR features.

Click **WIZARD SETUP** for initial configuration including general setup, wireless LAN setup, ISP Parameters for Internet Access and WAN IP/DNS/MAC Address Assignment.

Click the links under **ADVANCED** to configure advanced features such as **SYSTEM** (General Setup, Dynamic DNS, Password and Time Setting), **LAN** (DHCP and TCP/IP Setup), **WLAN** (WLAN and WLAN Security Setup), **WAN**, **SUA/NAT**, **STATIC ROUTE** (Route Entry), **FIREWALL** (Settings, Filter and Services), **Internal RADIUS Server** (Settings, Trusted AP and Trusted User databases), **CERTIFICATES** (My Certificates, Trusted CAs), **REMOTE MGNT** (Telnet, FTP, WWW, SNMP, DNS and Security), **UPnP** and **Logs** (View Log, Log Settings and Reports).

Click **MAINTENANCE** to view information about your ZyAIR or upgrade configuration/firmware files. Maintenance includes **Status** (Statistics), **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore and Default) and **Restart**

Click **LOGOUT** at any time to exit the web configurator

CHAPTER 3

Wizard Setup

The web configurator's setup wizard helps you configure your ZyAIR for Internet access and set up wireless LAN.

3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

3.1.1 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b and IEEE 802.11g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

3.1.2 ESS ID

An Extended Service Set (ESS) is a group of access points connected to a wired LAN on the same subnet. An ESS ID uniquely identifies each set. All access points and their associated wireless stations in the same set must have the same ESSID.

3.1.3 WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

3.1.4 WPA-PSK

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption. The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA - Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

3.2 Wizard Setup: General Setup

General Setup contains administrative and system-related information.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyAIR via DHCP.

Figure 5 Wizard 1 : General Setup

WIZARD SETUP

General Setup:
 This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name:

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

Domain Name:

Next

The following table describes the labels in this screen.

Table 3 Wizard 1 : General Setup

LABEL	DESCRIPTION
System Name	<p>It is recommended you type your computer's "Computer name".</p> <p>In Windows 95/98 click Start, Settings, Control Panel, Network. Click the Identification tab, note the entry for the Computer Name field and enter it as the System Name.</p> <p>In Windows 2000, click Start, Settings, Control Panel and then double-click System. Click the Network Identification tab and then the Properties button. Note the entry for the Computer name field and enter it as the System Name.</p> <p>In Windows XP, click Start, My Computer, View system information and then click the Computer Name tab. Note the entry in the Full computer name field and enter it as the ZyAIR System Name.</p> <p>This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.</p>
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Next	Click Next to proceed to the next screen.

3.3 Wizard Setup: Wireless LAN

Use the second wizard screen to set up the wireless LAN.

Figure 6 Wizard 2 : Wireless LAN Setup

The following table describes the labels in this screen.

Table 4 Wizard 2 : Wireless LAN Setup

LABEL	DESCRIPTION
Wireless LAN Setup	
ESSID	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyAIR, make sure all wireless stations use the same SSID in order to access the network.
Choose Channel ID	To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.
Security	The level of Security can be selected as none, basic or extended. Choose None security to have no wireless LAN security configured and proceed to the ISP Parameters for Internet Access screen. Choose Basic (WEP) security if you want to configure WEP Encryption parameters. Choose Extend (WPA-PSK) security to configure a Pre-Shared Key . The third screen varies depending on which security level you select.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.



Note: The wireless stations and ZyAIR must use the same ESSID, channel ID and WEP encryption key (if WEP is enabled) or WPA-PSK (if WPA-PSK is enabled) for wireless communication

3.4 Wizard Setup: Screen 3

Choose **Basic (WEP)** security to setup WEP Encryption parameters.

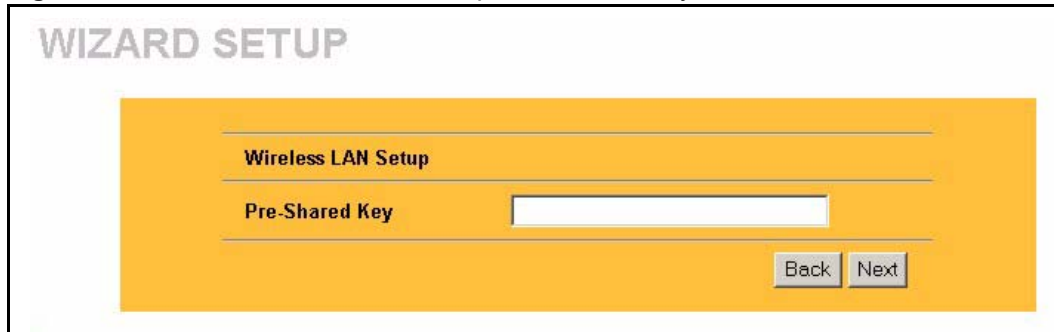
Figure 7 Wizard 3: Wireless LAN Setup: Basic Security

The following table describes the labels in this screen.

Table 5 Wizard 3: Wireless LAN Setup: Basic Security

LABEL	DESCRIPTION
Passphrase	You can generate or manually enter a WEP key by either: Entering a Passphrase (up to 32 printable characters) and clicking Generate . The Prestige automatically generates a WEP key. Or Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.
WEP Encryption	Select 64-bit WEP or 128-bit WEP to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). ZyAIRIf you chose 128-bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.

Choose **Extend (WPA-PSK)** security in the Wireless LAN Setup screen to set up a **Pre-Shared Key**.

Figure 8 Wizard 3: Wireless LAN Setup: Extend Security

The following table describes the labels in this screen.

Table 6 Wizard 3: Wireless LAN Setup: Extend Security

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the advanced wireless screen. You need to configure an authentication server to do this.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.

Refer to the chapter on wireless LAN for more information.

3.5 Wizard Setup: Screen 4

The ZyAIR offers three choices of encapsulation. They are **Ethernet**, **PPP over Ethernet** or **PPTP**.

3.5.1 Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 9 Wizard 4: Ethernet Encapsulation

WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: Ethernet

Service Type: Standard

User Name: N/A

Password: N/A

Login Server IP Address: N/A

Back Next

The following table describes the labels in this screen.

Table 7 Wizard 4: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet. Otherwise, choose PPP over Ethernet or PPTP for a dial-up connection.
Service Type	Choose from Standard , Telstra (RoadRunner Telstra authentication method), RR-Manager (Roadrunner Manager authentication method), RR-Toshiba (Roadrunner Toshiba authentication method) or Telia Login . The following fields are not applicable (N/A) for the Standard service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server	This field only applies when you select Telia Login in the Service Type field. Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Every (min)	This field only applies when you select Telia Login in the Service Type field. The Telia server logs the ZyAIR out if the ZyAIR does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyAIR to wait between logins.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.

3.5.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the ZyAIR (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyAIR does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

Figure 10 Wizard 4: PPPoE Encapsulation

The following table describes the labels in this screen.

Table 8 Wizard 4: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose PPP over Ethernet from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed-Up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is 100 seconds.
Next	Click Next to continue.
Back	Click Back to return to the previous screen.

3.5.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.



Note: The ZyAIR supports one PPTP server connection at any given time.

Figure 11 Wizard 4: PPTP Encapsulation

The following table describes the fields in this screen

Table 9 Wizard 4: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select PPTP from the drop-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed-Up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. The default is 100 seconds.
PPTP Configuration	

Table 9 Wizard 4: PPTP Encapsulation

LABEL	DESCRIPTION
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.

3.6 Wizard Setup: Screen 5

The fifth wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

3.6.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 10 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.



Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

3.6.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyAIR, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyAIR will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyAIR unless you are instructed to do otherwise.

3.6.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyAIR can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
- 2 If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

3.6.4 WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.



Note: ZyXEL recommends you clone the MAC address from a computer on your LAN even if your ISP does not require MAC address authentication.

Table 11 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(ZyAIR LAN IP)

The fifth wizard screen varies according to the type of encapsulation that you select in the third wizard screen.

Figure 12 Wizard 5: WAN Setup

WIZARD SETUP

WAN IP Address Assignment

☒ Get automatically from ISP (Default)
☐ Use fixed IP address

My WAN IP Address: 0.0.0.0
 My WAN IP Subnet Mask: 0.0.0.0
 Gateway IP Address: 0.0.0.0

DNS Server Address Assignment

First DNS Server: From ISP 0.0.0.0
 Second DNS Server: From ISP 0.0.0.0
 Third DNS Server: From ISP 0.0.0.0

WAN MAC Address

☒ Factory default
☐ Spoof this computer's MAC Address - IP Address: 192.168.1.2

Back Next

The following table describes the labels in this screen

Table 12 Wizard 5: WAN Setup

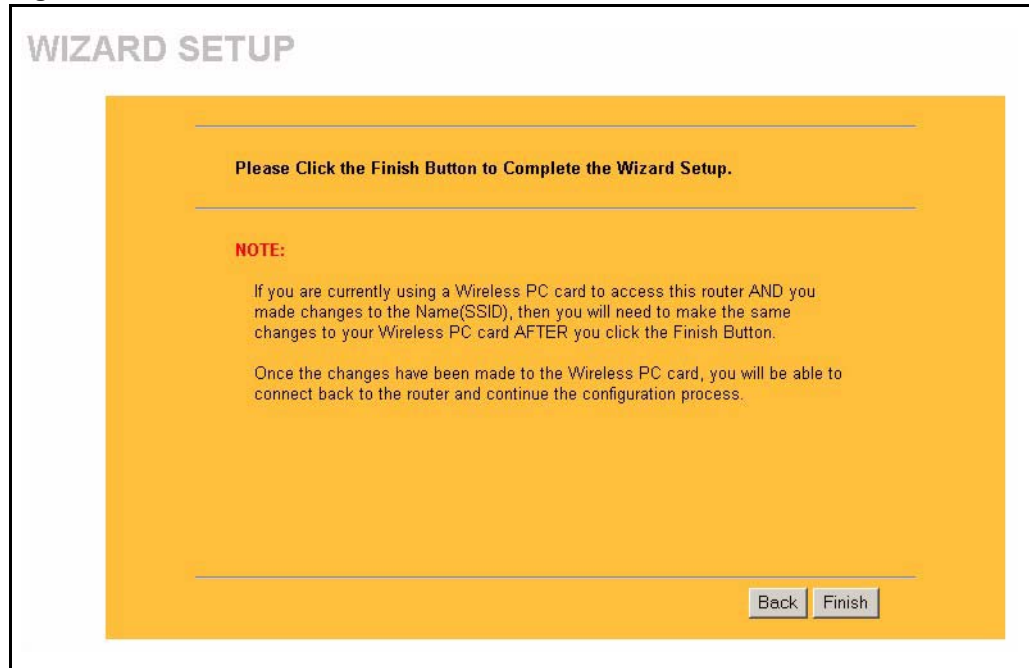
LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address. Enter a subnet mask appropriate to your network and the gateway IP address if applicable.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
My WAN IP Subnet Mask	Enter a Subnet Mask appropriate to your network. a
Gateway IP Address	Enter the Gateway IP Address of the neighboring device, if you know it. If you do not, leave the Gateway IP Address field as 0.0.0.0.
System DNS Server Address Assignment (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyAIR uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	

Table 12 Wizard 5: WAN Setup

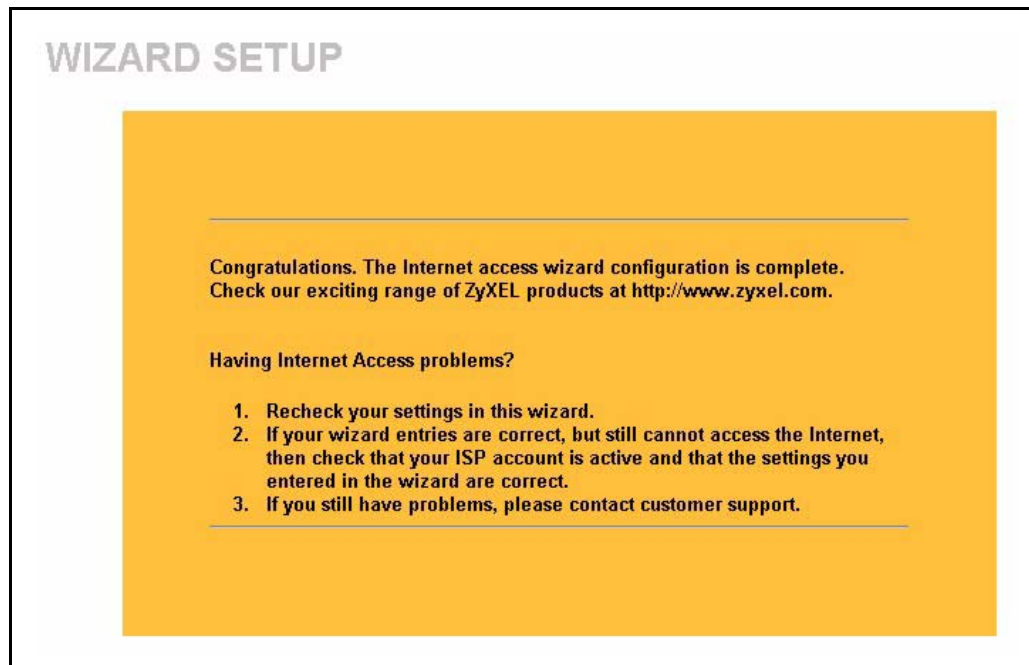
LABEL	DESCRIPTION
First DNS Server	Select From ISP if your ISP dynamically assigns DNS server information (and the ZyAIR's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select None if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Second DNS Server	
Third DNS Server	
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.

3.7 Basic Setup Complete

Click **Back** to return to the previous screen or click **Finish** to complete and save the wizard setup.

Figure 13 Wizard Finish

Well done! You have successfully set up the ZyAIR. A congratulations screen displays some information.



CHAPTER 4

System Screens

4.1 System Overview

This section provides information on general system setup.

4.2 Configuring General Setup

Click the **SYSTEM** link under **ADVANCED** to open the **General** screen.

Figure 14 System General Setup

SYSTEM

General DDNS Password Time Setting

System Name G-2000PLUS

Domain Name

Administrator Inactivity Timer 5 (minutes, 0 means no timeout)

System DNS Servers

First DNS Server From ISP 0.0.0.0

Second DNS Server From ISP 0.0.0.0

Third DNS Server From ISP 0.0.0.0

Apply Reset

The following table describes the labels in this screen.

Table 13 System General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Type a descriptive name to identify the ZyAIR in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.

Table 13 System General Setup

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select From DHCP if your DHCP server dynamically assigns DNS server information (and the ZyAIR's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is None .
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

4.3 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

4.3.1 DynDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.



Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

4.4 Configuring Dynamic DNS

To change your ZyAIR's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

Figure 15 DDNS

The following table describes the labels in this screen.

Table 14 DDNS

LABEL	DESCRIPTION
Enable DDNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when CustomDNS is selected in the DDNS Type field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	

Table 14 DDNS

LABEL	DESCRIPTION
Use WAN IP address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
DDNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
Use specified IP Address	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Address	Enter the IP address if you select the Use specified IP Address option.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

4.5 Configuring Password

To change your ZyAIR's password (recommended), click the **SYSTEM** link under **ADVANCED** and then the **Password** tab. The screen appears as shown. This screen allows you to change the ZyAIR's password.

If you forget your password (or the ZyAIR IP address), you will need to reset the ZyAIR. See the *Resetting the ZyAIR* section for details

Figure 16 Password.

The following table describes the labels in this screen.

Table 15 Password

LABEL	DESCRIPTIONS
Old Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

4.6 Configuring Time Setting

To change your ZyAIR's time and date, click the **SYSTEM** link under **ADVANCED** and then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the ZyAIR's time based on your local time zone.

Figure 17 Time Setting

The following table describes the labels in this screen.

Table 16 Time Setting

LABEL	DESCRIPTION
Time Protocol	<p>Select the time service protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.</p> <p>The main difference between them is the format.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, NTP (RFC 1305), is similar to Time (RFC 868).</p> <p>Select None to enter the time and date manually.</p>
Time Server Address	Enter the IP address or the URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time (hh:mm:ss)	<p>This field displays the time of your ZyAIR.</p> <p>Each time you reload this page, the ZyAIR synchronizes the time with the time server.</p>

Table 16 Time Setting

LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server. When you select None in the Time Protocol field, enter the new time in this field and then click Apply .
Current Date (yyyy/mm/dd)	This field displays the date of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the date with the time server.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server. When you select None in the Time Protocol field, enter the new date in this field and then click Apply .
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date (mm-dd)	Enter the month and day that your daylight-savings time starts on if you selected Daylight Savings .
End Date (mm-dd)	Enter the month and day that your daylight-savings time ends on if you selected Daylight Savings .
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

CHAPTER 5

LAN Screens

This chapter describes how to configure LAN settings.

5.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

5.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyAIR as a DHCP server or disable it. When configured as a server, the ZyAIR provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

5.2.1 IP Pool Setup

The ZyAIR is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyAIR itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

5.2.2 System DNS Servers

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter.

5.3 LAN TCP/IP

The ZyAIR has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

5.3.1 Factory LAN Defaults

The LAN parameters of the ZyAIR are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

5.3.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

5.3.3 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyAIR will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the ZyAIR sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

5.3.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address

224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyAIR supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyAIR queries all directly connected networks to gather group membership. After that, the ZyAIR periodically updates this information. IP multicasting can be enabled/disabled on the ZyAIR LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

5.4 Configuring IP

Click **LAN** to open the **IP** screen.

Figure 18 LAN IP

The following table describes the labels in this screen.

Table 17 LAN IP

LABEL	DESCRIPTION
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the DHCP Server check box selected unless your ISP instructs you to do otherwise. Clear it to disable the ZyAIR acting as a DHCP server. When configured as a server, the ZyAIR provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Servers Assigned by DHCP Server The ZyAIR passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The ZyAIR only passes this information to the LAN DHCP clients when you select the DHCP Server check box. When you clear the DHCP Server check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.	

Table 17 LAN IP

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the ZyAIR's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select DNS Relay to have the ZyAIR act as a DNS proxy. The ZyAIR's LAN IP address displays in the field to the right (read-only). The ZyAIR tells the DHCP clients on the LAN that the ZyAIR itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyAIR, the ZyAIR forwards the query to the ZyAIR's system DNS server (configured in the SYSTEM General screen) and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
LAN TCP/IP	
IP Address	Type the IP address of your ZyAIR in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the ZyAIR will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received. Both is the default.
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyAIR sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Multicast	Select IGMP V-1 or IGMP V-2 or None . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	

Table 17 LAN IP

LABEL	DESCRIPTION
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

5.5 Configuring Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your ZyAIR's Static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown.

Figure 19 Static DHCP

LAN

IPStatic DHCPIP Alias

#	MAC Address	IP Address
1		0.0.0.0
2		0.0.0.0
3		0.0.0.0
4		0.0.0.0
5		0.0.0.0
6		0.0.0.0
7		0.0.0.0
8		0.0.0.0

ApplyReset

The following table describes the labels in this screen.

Table 18 Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	This field specifies the size, or count of the IP address pool.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

5.6 Configuring IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network.

To change your ZyAIR's IP Alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

Figure 20 IP Alias

LAN IP SETUP

IP Static DHCP **IP Alias**

☐ IP Alias 1

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

RIP Direction: None

RIP Version: RIP-1

☐ IP Alias 2

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

RIP Direction: None

RIP Version: RIP-1

Apply Reset

The following table describes the labels in this screen.

Table 19 IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the ZyAIR.
IP Address	Enter the IP address of your ZyAIR in dotted decimal notation.
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the ZyAIR will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyAIR sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 6

Wireless Configuration and Roaming

This chapter discusses how to configure the Wireless and Roaming screens on the ZyAIR.

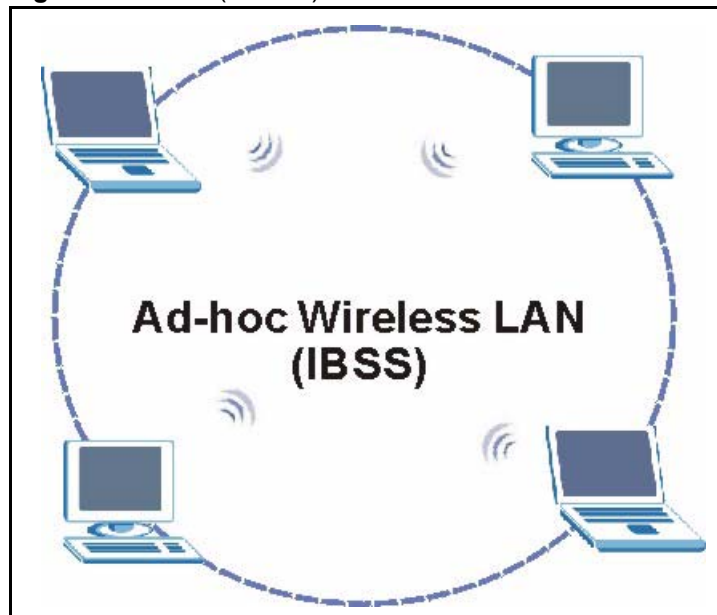
6.1 Wireless LAN Overview

This section introduces the wireless LAN(WLAN) and some basic scenarios.

6.1.1 IBSS

An Independent Basic Service Set (IBSS), also called an Ad-hoc network, is the simplest WLAN configuration. An IBSS is defined as two or more computers with wireless adapters within range of each other that form an independent (wireless) network without the need of an access point (AP).

Figure 21 IBSS (Ad-hoc) Wireless LAN

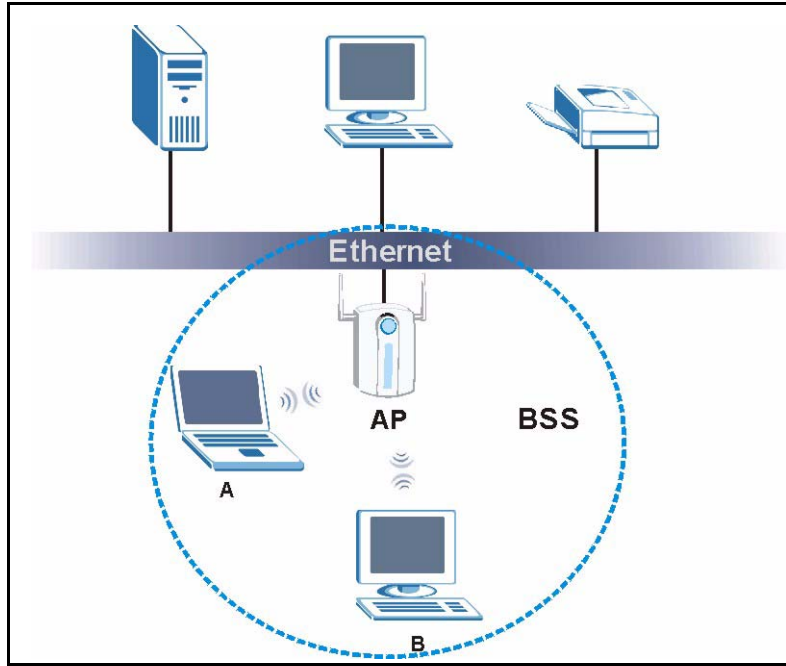


6.1.2 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

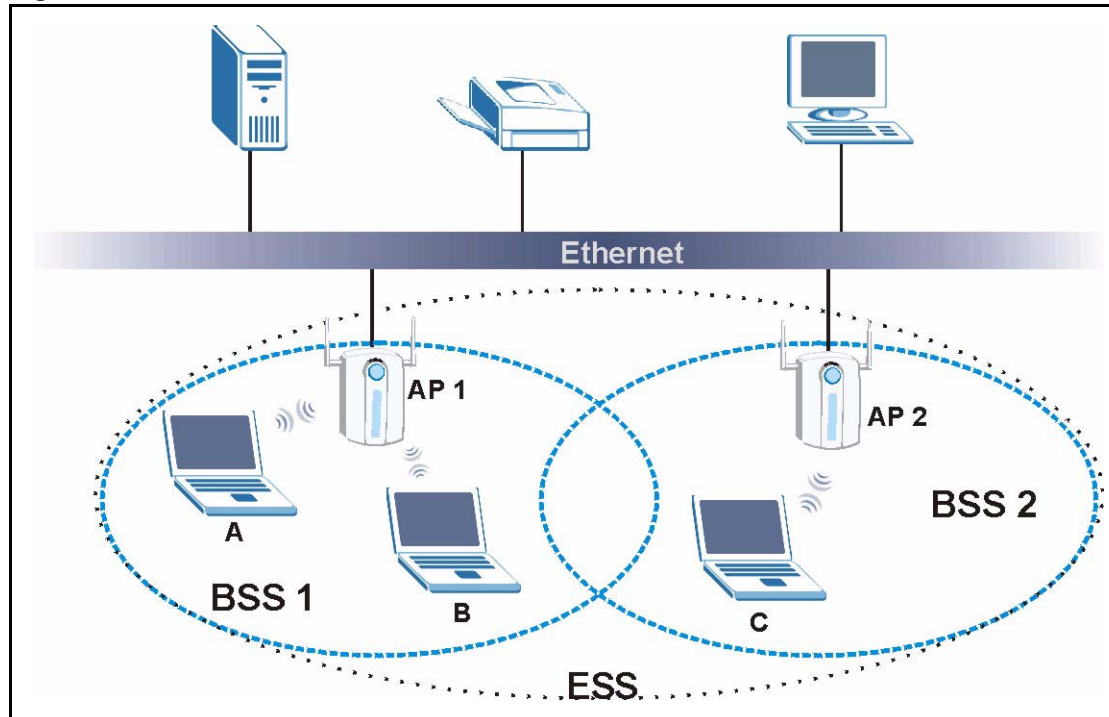
Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 22 Basic Service set



6.1.3 ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). An ESSID (ESS Identification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

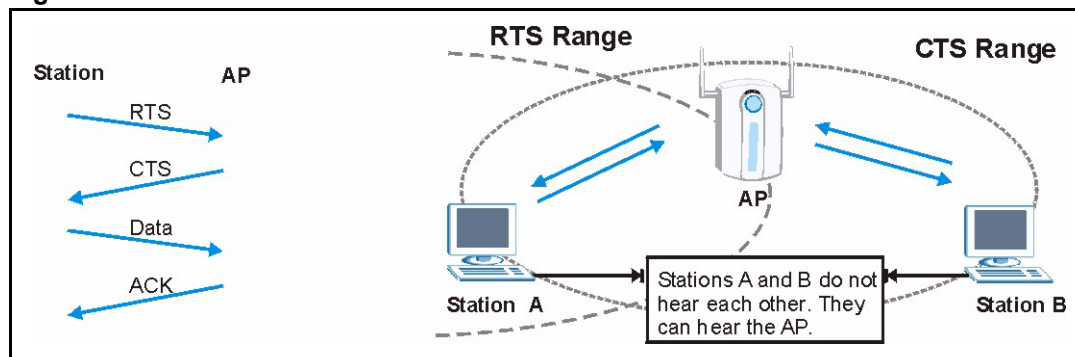
Figure 23 Extended Service Set

6.2 Wireless LAN Basics

Refer also to the *Wizard Setup* chapter for more background information on Wireless LAN features, such as channels.

6.2.1 RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot “hear” each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 24 RTS/CTS

When station A sends data to the ZyAIR, it might not know that station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the “cost” of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.



Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Note:

6.2.2 Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyAIR will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set, then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

6.3 Configuring Wireless



Note: If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings.

Click the **WIRELESS** link under **ADVANCED** to open the **Wireless** screen.

Figure 25 Wireless

The following table describes the general wireless LAN labels in this screen.

Table 20 Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
ESSID	(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings.
Hide ESSID	Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning using a site survey tool.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. Refer to the <i>Wizard Setup</i> chapter for more information on channels.
RTS/CTS Threshold	Enter a value between 0 and 2432. The default is 2432 .
Fragmentation Threshold	Enter a value between 256 and 2432. The default is 2432 . It is the maximum data fragment size that can be sent.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

See the *Wireless Security* chapter for information on the other labels in this screen.

6.4 Configuring Roaming

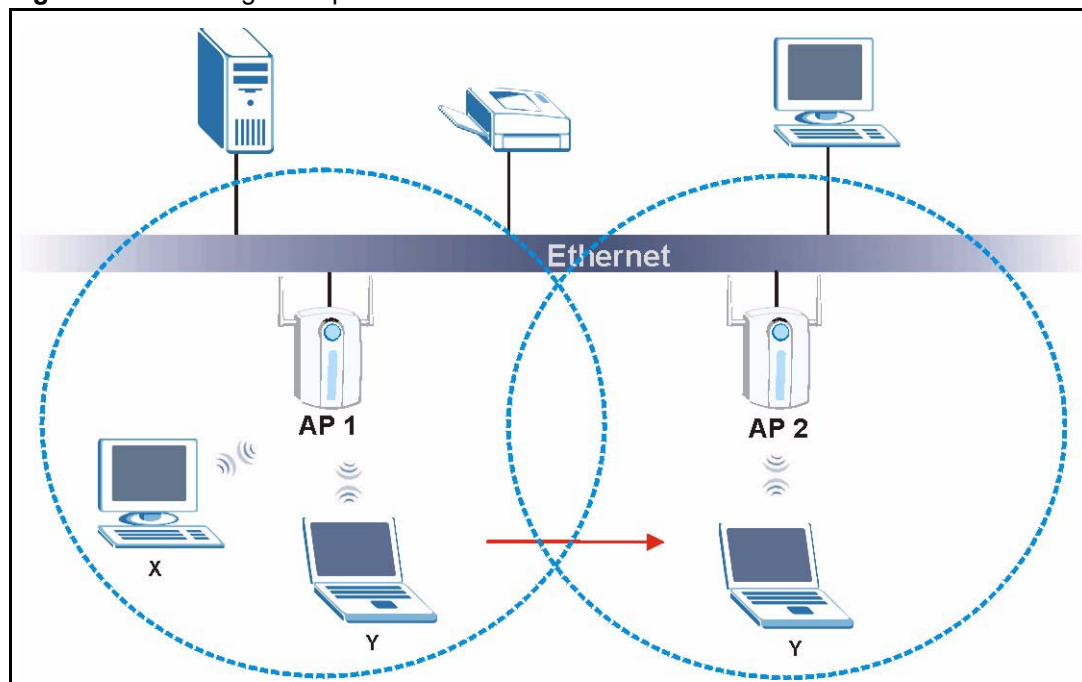
A wireless station is a device with an IEEE 802.11mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in [see Figure 26](#).

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

Figure 26 Roaming Example



The steps below describe the roaming process.

- 1** As wireless station **Y** moves from the coverage area of access point **P1** to that of access point
- 2 P2**, it scans and uses the signal of access point **P2**.
- 3** Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.
- 4** Access point **P1** updates the new position of wireless station.
- 5** Wireless station **Y** sends a request to access point **P2** for re-authentication.

6.4.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

- 1** All the access points must be on the same subnet and configured with the same ESSID.
- 2** If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
- 3** The adjacent access points should use different radio channels when their coverage areas overlap.
- 4** All access points must use the same port number to relay roaming information.
- 5** The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your ZyAIR, click the **WIRELESS** link under **ADVANCED** and then the **Roaming** tab. The screen appears as shown.

Figure 27 Roaming

The screenshot shows the 'WIRELESS LAN' configuration page. The 'Roaming' tab is active. The 'Roaming Configuration' section contains the following fields:

- Active:** A dropdown menu currently set to 'No'.
- Port:** A text input field containing the value '3517'.

At the bottom of the configuration area are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 21 Roaming

LABEL	DESCRIPTION
Active	Select Yes from the drop-down list box to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming.
Port	Enter the port number to communicate roaming information between APs. The port number must be the same on all APs. The default is 3517. Make sure this port is not used by other services.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

CHAPTER 7

Wireless Security

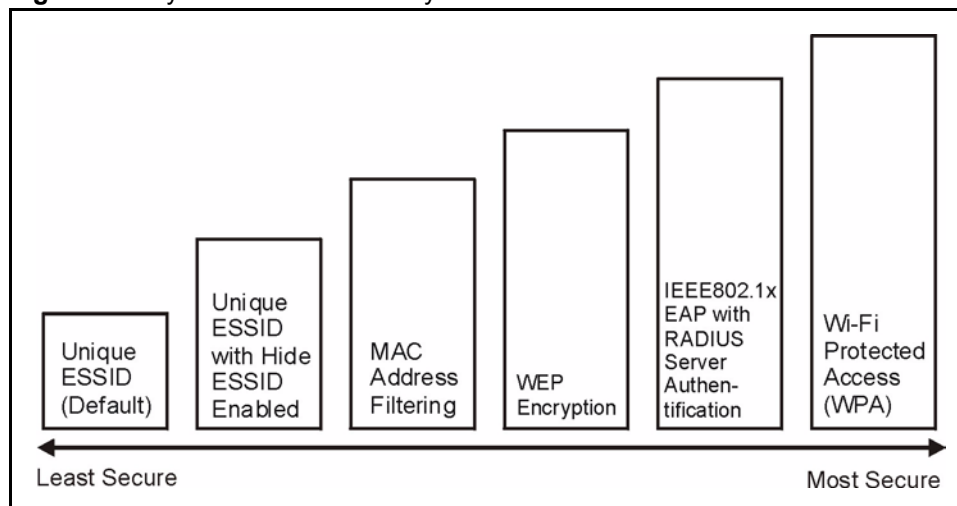
This Chapter describes how to use the MAC Filter, 802.1x, Roaming and RADIUS to configure wireless security on your ZyAIR.

7.1 Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless stations, access points and the wired network.

The figure below shows the possible wireless security levels on your ZyAIR. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

Figure 28 ZyAIR Wireless Security Levels



If you do not enable any wireless security on your ZyAIR, your network is accessible to any wireless networking device that is within range.

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

Figure 29 Wireless: No Security

The screenshot shows the 'WIRELESS LAN' configuration interface. At the top, there are three tabs: 'Wireless' (selected), 'MAC Filter', and 'Roaming'. Below the tabs, the 'Enable Wireless LAN' checkbox is checked. The 'ESSID' is set to 'Wireless'. The 'Hide ESSID' checkbox is unchecked. The 'Choose Channel ID' dropdown is set to 'Channel-06 2437MHz'. The 'RTS/CTS Threshold' is set to '2432' (range 0 ~ 2432). The 'Fragmentation Threshold' is set to '2432' (range 256 ~ 2432). The 'Security' dropdown is set to 'No Security'. The 'Enable Breathing LED' checkbox is checked. The 'Preamble' dropdown is set to 'Long'. The '802.11 Mode' dropdown is set to 'Mixed'. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 22 Wireless No Security

LABEL	DESCRIPTION
Security	Choose from one of the security features listed in the drop-down box. <ul style="list-style-type: none"> No Security Static WEP WPA-PSK WPA 802.1x + Dynamic WEP 802.1x + Static WEP 802.1x + No WEP
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.
Preamble	Select a preamble type from the drop-down list menu. Choices are Long , Short and Dynamic . See the section on preamble for more information.
802.11 Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR. Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.2 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 23 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Enable
WPA	TKIP	No	Enable
WPA-PSK	WEP	Yes	Enable
WPA-PSK	TKIP	Yes	Enable

7.3 WEP Overview

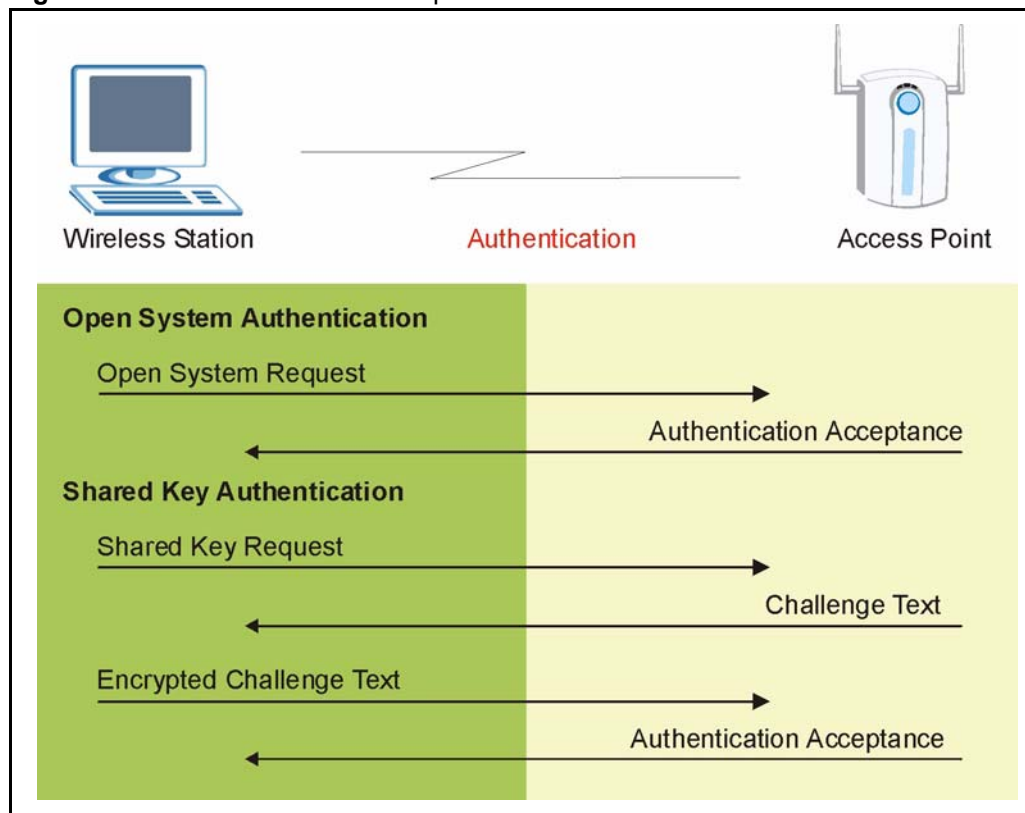
WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

7.3.1 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your ZyAIR allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

7.3.1.1 Authentication

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.

Figure 30 WEP Authentication Steps

Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your ZyAIR's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the ZyAIR will accept either type of authentication request and the ZyAIR will fall back to use open authentication if the shared key does not match.

7.4 Configuring WEP Encryption

In order to configure and enable WEP encryption; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **Static WEP** from the **Security** list.

Figure 31 Wireless: Static WEP Encryption

The screenshot shows the 'WIRELESS LAN' configuration page with three tabs: 'Wireless', 'MAC Filter', and 'Roaming'. The 'Wireless' tab is active. The 'Enable Wireless LAN' checkbox is checked. The 'ESSID' is set to 'Wireless'. The 'Hide ESSID' checkbox is unchecked. The 'Choose Channel ID' is set to 'Channel-06 2437MHz'. The 'RTS/CTS Threshold' is set to '2432' (0 ~ 2432). The 'Fragmentation Threshold' is set to '2432' (256 ~ 2432). The 'Security' dropdown is set to 'Static WEP'. The 'Passphrase' field is empty, and the 'Generate' button is visible. The 'WEP Encryption' dropdown is set to '64-bit WEP'. The 'Authentication Method' dropdown is set to 'Auto'. Below this, there are instructions for 64-bit and 128-bit WEP. The 'ASCII' radio button is selected, and the 'Hex' radio button is unselected. There are four 'Key' fields (Key 1, Key 2, Key 3, Key 4) with corresponding radio buttons. The 'Enable Breathing LED' checkbox is checked. The 'Preamble' dropdown is set to 'Long'. The '802.11 Mode' dropdown is set to 'Mixed'. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the wireless LAN security labels in this screen.

Table 24 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Passphrase	Enter a Passphrase (up to 32 printable characters) and click Generate . The ZyAIR automatically generates a WEP key.
WEP Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	This field is activated when you select 64-bit WEP or 128-bit WEP in the WEP Encryption field. Select Auto , Open System or Shared Key from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option in order to enter hexadecimal characters as the WEP keys. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

Table 24 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>
Enable Breathing LED	<p>Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations.</p> <p>Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.</p>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are Long, Short and Dynamic.</p> <p>See the section on preamble for more information.</p>
802.11 Mode	<p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR.</p> <p>Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.</p>
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.5 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

7.5.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. See [“Internal RADIUS Server” on page 114](#) for more information on authentication of Trusted User's. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS, EAP and PEAP.

If you don't have an external RADIUS server you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

7.5.2 Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

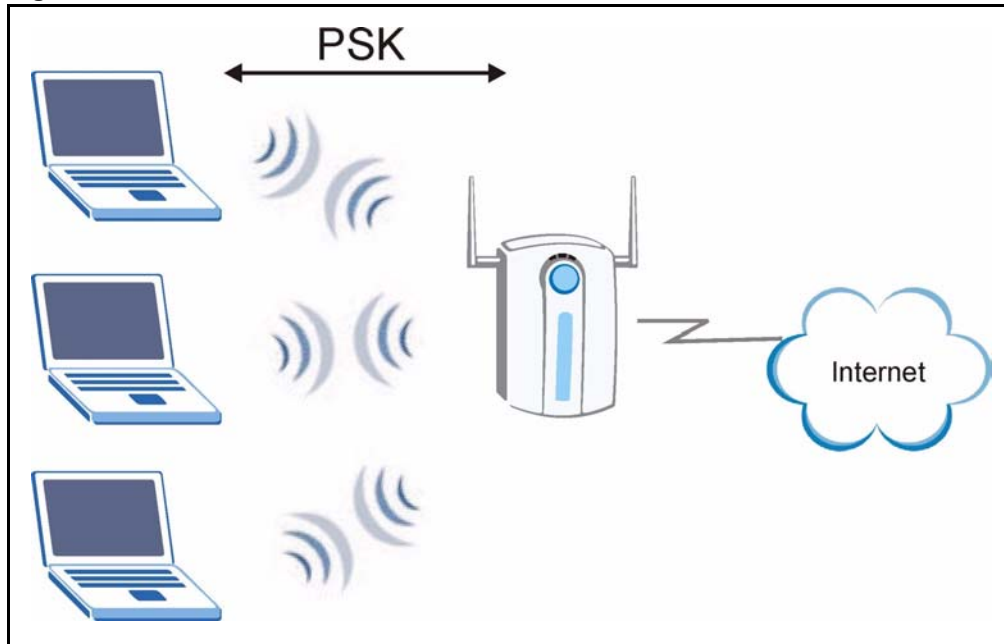
By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

7.5.3 WPA-PSK Application Example

A WPA-PSK application looks as follows.

- 1** First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2** The AP checks each client's password and (only) allows it to join the network if it matches its password.
- 3** The AP derives and distributes keys to the wireless clients.
- 4** The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 32 WPA - PSK Authentication

7.6 Configuring WPA-PSK Authentication

In order to configure and enable WPA-PSK Authentication; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **WPA-PSK** from the **Security** list.

Figure 33 Wireless: WPA-PSK

WIRELESS LAN

Wireless | MAC Filter | Roaming

☒ Enable Wireless LAN

ESSID: Wireless

☐ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: WPA-PSK

Pre-Shared Key: [Text Field]

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

WPA Group Key Update Timer: 1800 (In Seconds)

☒ Enable Breathing LED

Preamble: Long

802.11 Mode: Mixed

Apply Reset

The following table describes the labels in this screen.

Table 25 Wireless: WPA-PSK

LABEL	DESCRIPTION
Pre-Shared Key	<p>The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials.</p> <p>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).</p>
ReAuthentication Timer (in seconds)	<p>Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Idle Timeout	<p>The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).</p>
WPA Group Key Update Timer	<p>The WPA Group Key Update Timer is the rate at which the AP (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the WPA Group Key Update Timer is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).</p>

Table 25 Wireless: WPA-PSK

LABEL	DESCRIPTION
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.
Preamble	Select a preamble type from the drop-down list menu. Choices are Long , Short and Dynamic . See the section on preamble for more information.
802.11 Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR. Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.7 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

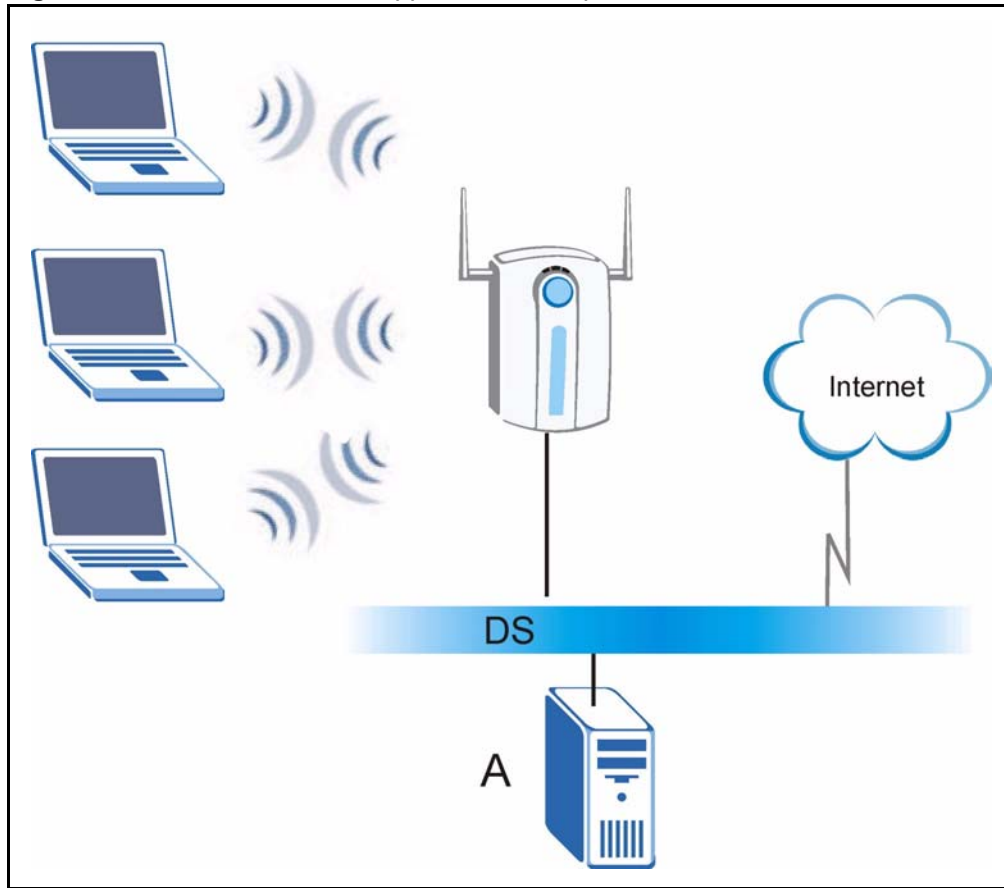
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

The Funk Software's Odyssey client is bundled free (at the time of writing) with the client wireless adaptor(s).

7.7.1 WPA with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 34 WPA with RADIUS Application Example

7.8 Configuring WPA Authentication

In order to configure and enable WPA Authentication; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **WPA** from the **Security** list.

Figure 35 Wireless: WPA

The screenshot shows the 'WIRELESS LAN' configuration page with three tabs: 'Wireless', 'MAC Filter', and 'Roaming'. The 'Wireless' tab is active. The page has an orange background and contains the following settings:

- ☒ **Enable Wireless LAN**
- ESSID**: Wireless
- ☐ **Hide ESSID**
- Choose Channel ID**: Channel-06 2437MHz
- RTS/CTS Threshold**: 2432 (0 ~ 2432)
- Fragmentation Threshold**: 2432 (256 ~ 2432)
- Security**: WPA
- ReAuthentication Timer**: 1800 (In Seconds)
- Idle Timeout**: 3600 (In Seconds)
- WPA Group Key Update Timer**: 1800 (In Seconds)
- ☐ **Internal RADIUS Server**
- ☒ **External RADIUS Server**
 - Authentication Server**
 - IP Address**: 0.0.0.0
 - Port Number**: 1812
 - Shared Secret**: [Empty field]
 - Accounting Server**
 - ☐ **Active**
 - IP Address**: 0.0.0.0
 - Port Number**: 1813
 - Shared Secret**: [Empty field]
- ☒ **Enable Breathing LED**
- Preamble**: Long
- 802.11 Mode**: Mixed

At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 26 Wireless: WPA

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

Table 26 Wireless: WPA

LABEL	DESCRIPTION
WPA Group Key Update Timer	The WPA Group Key Update Timer is the rate at which the AP (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the WPA Group Key Update Timer is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.9 Introduction to RADIUS

RADIUS is based on a client-server model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- Authentication
Determines the identity of the users.
- Accounting
Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your ZyAIR acts as a message relay between the wireless station and the network RADIUS server.

7.9.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.

7.9.1.1 Access-Challenge

Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

7.9.1.2 Accounting-Request

Sent by the access point requesting accounting.

7.9.1.3 Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the wired network from unauthorized access.

7.9.1.4 EAP Authentication Overview

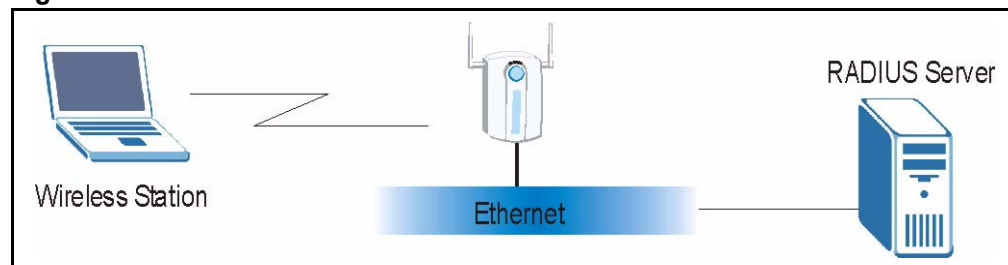
EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The ZyAIR supports EAP-TLS, EAP-TTLS and PEAP with RADIUS. Refer to the *Types of EAP Authentication* appendix for descriptions on the common types.

Your ZyAIR supports PEAP with the Internal RADIUS Server.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

Figure 36 EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of PEAP authentication steps, see the IEEE 802.1x appendix.

- 1 The wireless station sends a “start” message to the ZyAIR.
- 2 The ZyAIR sends a “request identity” message to the wireless station for identity information.
- 3 The wireless station replies with identity information, including username and password.

- 4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

7.10 Configuring RADIUS

You can configure the ZyAIR to authenticate wireless clients using an external RADIUS server or have the ZyAIR itself act as a RADIUS server using the internal RADIUS server.

To specify a RADIUS server, click the **WIRELESS** link under **ADVANCED** and then choose **Internal RADIUS Server** or **External RADIUS Server** in the Wireless configuration screen. The screen appears as shown. See [Chapter 8, "Internal RADIUS Server"](#) for more details on RADIUS.

Figure 37 Wireless: WPA

WIRELESS LAN

Wireless MAC Filter Roaming

☒ Enable Wireless LAN

ESSID: Wireless

☐ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: WPA

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

WPA Group Key Update Timer: 1800 (In Seconds)

☐ Internal RADIUS Server

☒ External RADIUS Server

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

Accounting Server

☐ Active

IP Address: 0.0.0.0

Port Number: 1813

Shared Secret:

☒ Enable Breathing LED

Preamble: Long

802.11 Mode: Mixed

Apply Reset

The following table describes the labels in this screen.

Table 27 RADIUS

LABEL	DESCRIPTION
Internal RADIUS Server	Select this radio button to use the ZyAIR's Internal RADIUS Server . You can authenticate other AP's or wireless clients in other wireless networks.
External RADIUS Server	Select the radio button to use an External RADIUS Server to authenticate the ZyAIR's wireless clients.
Authentication Server	
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.

Table 27 RADIUS

LABEL	DESCRIPTION
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyAIR. The key must be the same on the external authentication server and your ZyAIR. The key is not sent over the network.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is 1813 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyAIR. The key must be the same on the external accounting server and your ZyAIR. The key is not sent over the network.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.11 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the trusted user database internal to the ZyAIR (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

See also the section on RADIUS in this *User's Guide*.

7.12 Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

To use Dynamic WEP, enable and configure the RADIUS server and enable Dynamic WEP Key Exchange in the Wireless screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP



Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

7.13 Configuring 802.1x and Dynamic WEP Key Exchange

In order to configure and enable 802.1x and Dynamic WEP Key Exchange; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + Dynamic WEP** from the **Security** list.

Figure 38 Wireless: 802.1x and Dynamic WEP

WIRELESS LAN

Wireless | **MAC Filter** | **Roaming**

☒ **Enable Wireless LAN**

ESSID:

☐ **Hide ESSID**

Choose Channel ID:

RTS/CTS Threshold: (0 ~ 2432)

Fragmentation Threshold: (256 ~ 2432)

Security:

ReAuthentication Timer: (In Seconds)

Idle Timeout: (In Seconds)

Dynamic WEP Key Exchange:

☐ Internal RADIUS Server

☒ External RADIUS Server

Authentication Server

IP Address:

Port Number:

Shared Secret:

Accounting Server

☐ Active

IP Address:

Port Number:

Shared Secret:

☒ **Enable Breathing LED**

Preamble:

802.11 Mode:

The following table describes the labels in this screen.

Table 28 Wireless: 802.1x and Dynamic WEP

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Dynamic WEP Key Exchange	Select 64-bit WEP or 128-bit WEP to enable data encryption. Up to 32 stations can access the ZyAIR when you configure dynamic WEP key exchange. This field is not available when you set Security to WPA or WPA-PSK .

Table 28 Wireless: 802.1x and Dynamic WEP

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.14 Configuring 802.1x and Static WEP Key Exchange

In order to configure and enable 802.1x and Static WEP Key Exchange; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + Static WEP** from the **Security** list.

Figure 39 Wireless: 802.1x and Static WEP

WIRELESS LAN

Wireless **MAC Filter** Roaming

☒ **Enable Wireless LAN**

ESSID: Wireless

☐ **Hide ESSID**

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: 802.1x + Static WEP

Passphrase: **Generate**

WEP Encryption: 64-bit WEP

Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

☒ ASCII ☐ Hex

☒ **Key 1**

☐ **Key 2**

☐ **Key 3**

☐ **Key 4**

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Authentication Databases: Local User Database Only

☐ Internal RADIUS Server

☒ **External RADIUS Server**

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

Accounting Server

☐ Active

IP Address: 0.0.0.0

Port Number: 1813

Shared Secret:

☒ **Enable Breathing LED**

Preamble: Long

802.11 Mode: Mixed

Apply **Reset**

The following table describes the labels in this screen.

Table 29 Wireless: 802.1x and Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a Passphrase (up to 32 printable characters) and click Generate . The ZyAIR automatically generates a WEP key.
WEP Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.

Table 29 Wireless: 802.1x and Static WEP

LABEL	DESCRIPTION
Authentication Method	This field is activated when you select 64-bit WEP or 128-bit WEP in the WEP Encryption field. Select Auto, Open System or Shared Key from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option in order to enter hexadecimal characters as the WEP keys. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>
ReAuthentication Timer (in seconds)	<p>Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Idle Timeout	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Authentication Databases	<p>The authentication database contains wireless station login information. The trusted user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local User Database Only to have the ZyAIR just check the built-in user trusted user database on the ZyAIR for a wireless station's username and password.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select Local first, then RADIUS to have the ZyAIR first check the trusted user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server.</p> <p>Select RADIUS first, then Local to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the trusted user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the trusted user database and the authentication fails.</p>
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.15 Configuring 802.1x

In order to configure and enable 802.1x; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + No WEP** from the **Security** list.

Figure 40 Wireless: 802.1x

WIRELESS LAN

Wireless **MAC Filter** Roaming

☒ **Enable Wireless LAN**

ESSID:

☐ **Hide ESSID**

Choose Channel ID:

RTS/CTS Threshold: (0 ~ 2432)

Fragmentation Threshold: (256 ~ 2432)

Security:

ReAuthentication Timer: (In Seconds)

Idle Timeout: (In Seconds)

Authentication Databases

☐ Internal RADIUS Server

☒ External RADIUS Server

Authentication Server

IP Address:

Port Number:

Shared Secret:

Accounting Server

☐ Active

IP Address:

Port Number:

Shared Secret:

☒ **Enable Breathing LED**

Preamble:

802.11 Mode:

The following table describes the labels in this screen.

Table 30 Wireless: 802.1x and No WEP

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

Table 30 Wireless: 802.1x and No WEP

LABEL	DESCRIPTION
Authentication Databases	<p>The authentication database contains wireless station login information. The trusted user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local User Database Only to have the ZyAIR just check the built-in trusted user database on the ZyAIR for a wireless station's username and password.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select Local first, then RADIUS to have the ZyAIR first check the trusted user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server.</p> <p>Select RADIUS first, then Local to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the trusted user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the trusted user database and the authentication fails.</p>
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

7.16 MAC Filter

The MAC filter screen allows you to configure the ZyAIR to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the ZyAIR (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your ZyAIR's MAC filter settings, click the **WIRELESS** link under **ADVANCED** and then the **MAC Filter** tab. The screen appears as shown.

Figure 41 MAC Address Filter

WIRELESS LAN

Wireless MAC Filter Roaming

MAC Address Filter

Active: No

Filter Action: Allow Association

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

Apply Reset

The following table describes the labels in this menu.

Table 31 MAC Address Filter

LABEL	DESCRIPTION
Active	Select Yes from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Address table. Select Deny Association to block access to the ZyAIR, MAC addresses not listed will be allowed to access the ZyAIR. Select Allow Association to permit access to the ZyAIR, MAC addresses not listed will be denied access to the ZyAIR.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the ZyAIR in these address fields.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

CHAPTER 8

Internal RADIUS Server

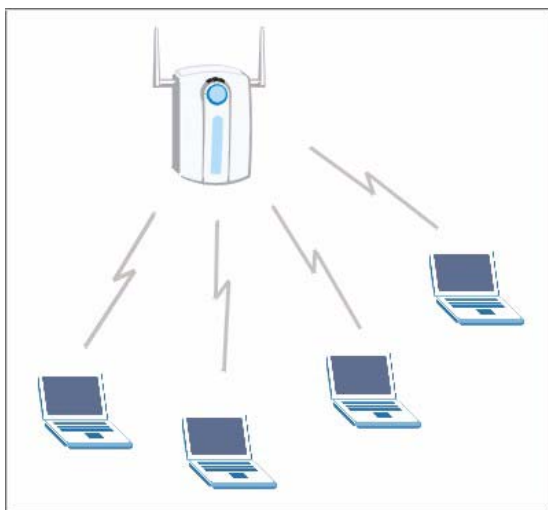
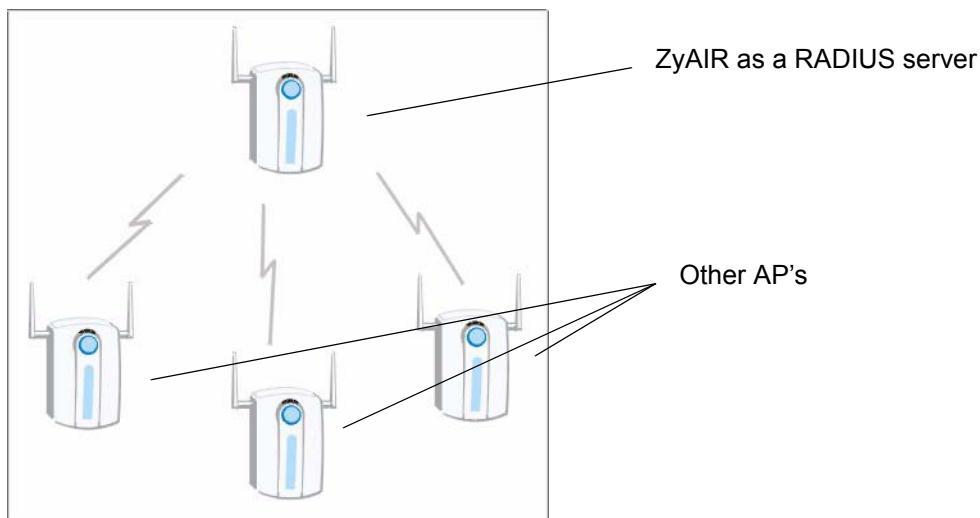
This chapter describes how to use the internal RADIUS server to authenticate wireless clients or other AP's in other wireless networks. For more background information on RADIUS, see [section 7.9](#).

8.1 Internal RADIUS Overview

The ZyAIR has a built-in RADIUS server that can authenticate wireless clients or other AP's in other wireless networks.

The ZyAIR can function as an AP and as a RADIUS server at the same time.

PEAP (Protected EAP) and MD5 authentication is implemented on the internal RADIUS server using simple username and password methods over a secure TLS connection. See the *Appendix* for more information on the types of EAP authentication and the internal RADIUS authentication method used in your ZyAIR.

Figure 42 ZyAIR Authenticates Wireless Stations**Figure 43** ZyAIR Authenticates other AP's**Table 32** Internal RADIUS Server

LABEL	DESCRIPTION
Setting	Use the Setting screen to display information about the ZyAIR's certificate and to activate the internal RADIUS server on your ZyAIR.
Trusted AP	Use the Trusted AP screen to configure which trusted AP's you can authenticate. You can authenticate up to 31 AP's using the ZyAIR's internal RADIUS.
Trusted Users	Use the Trusted Users screen to configure which wireless stations you can authenticate. The ZyAIR internal RADIUS server can authenticate up to 32 wireless clients..

8.2 Internal RADIUS Server Setting

The **INTERNAL RADIUS SERVER Setting** screen displays information about certificates. The certificates are used by wireless clients to authenticate the RADIUS server. Information matching the certificate is held on the wireless clients utility, for example, Funk Software's Odyssey client. A password and user name on the utility must match the the **Trusted Users** list so that the RADIUS server can be authenticated.

ZyXEL recommends that you replace the factory default certificate with one that uses your ZyAIR's MAC address. This can be done when you first log in to the ZyAIR or in the **Advanced** web configurator **Certificates** screen.



Note: The internal RADIUS server does not support domain accounts (DOMAIN/user). When you configure your Windows XP SP2 Wireless Zero Configuration PEAP/MS-CHAPv2 settings, deselect the **Use Windows logon name and password** checkbox. When authentication begins, a pop-up dialog box requests you to type a **Name**, **Password** and **Domain** of the RADIUS server. Specify a **Name** and **Password** only, do not specify a domain.

Refer to the *My Certificates* section in the *Certifications* chapter for information on how to replace, add or remove certificates.

Click the **AUTH SERVER** link under **ADVANCED** and then the **Setting** tab. The screen appears as shown.

Figure 44 Internal RADIUS Server Setting Screen

#	Name	Type	Subject	Issuer	Valid From	Valid To
1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-2000PLUS Factory Default Certificate	CN=ZyAIR G-2000PLUS Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

The following table describes the labels in this screen.

Table 33 My Certificates

LABEL	DESCRIPTION
Active	Select the Active checkbox to have the ZyAIR use its internal RADIUS server to authenticate wireless clients or other AP's.
#	This field displays the certificate index number. The certificates are listed in alphabetical order. Certificates can be added or removed in the Advanced Certificate screens. The internal RADIUS server uses one of the certificates listed in this screen to authenticate each wireless client. The exact certificate used, depends on the certificate information configured on the wireless client.
Name	This field displays the name used to identify this certificate. The ZyAIR has an auto_generated_self_signed_cert by factory default. The factory default certificate is common to all ZyAIR's that use certificates. You can replace the certificate when you log into the ZyAIR, see the section <i>Introducing the Web Configurator</i> or you can go to the Certificates configuration screen, see the <i>Certificates</i> chapter.
Type	<p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>*SELF represents the default self-signed certificate, which the ZyAIR uses to sign imported trusted remote host certificates.</p> <p>CERT represents a certificate issued by a certification authority.</p>
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

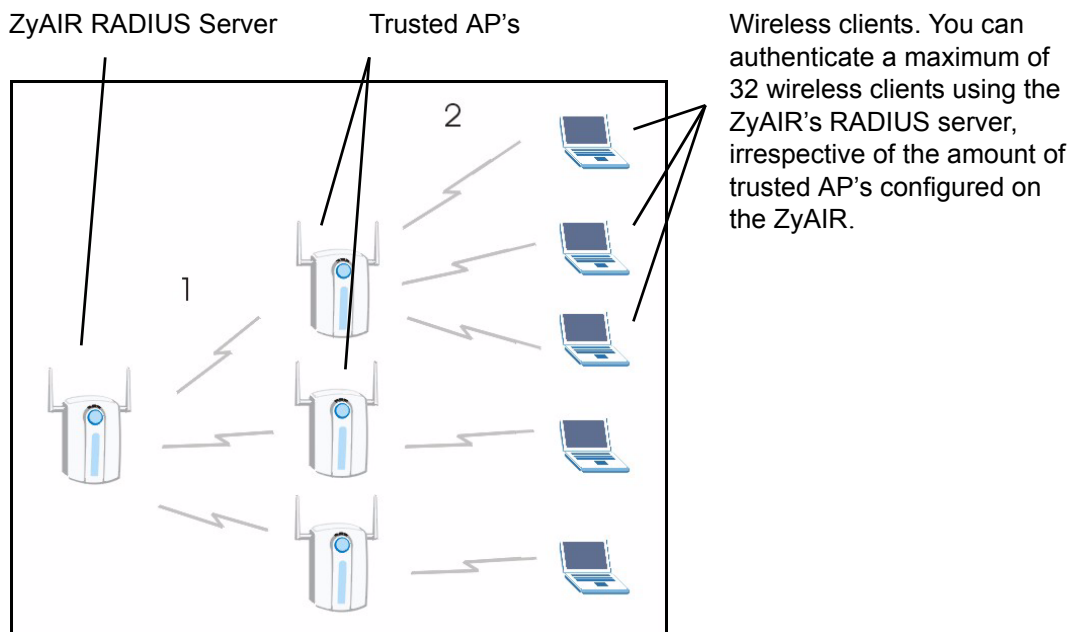
Table 33 My Certificates (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Apply	Click Apply to have the ZyAIR use certificates to authenticate wireless clients.
Reset	Click Reset to start configuring this screen afresh.

8.3 Trusted AP Overview

A trusted AP is an AP that uses the ZyAIR's internal RADIUS server to authenticate its wireless clients.

The following shows how this is done in two phases.

Figure 45 Trusted AP Overview

- 1 Configure an IP address and shared secret in the **Trusted AP** database to authenticate an AP as a trusted AP.

- 2 Configure wireless client user names and passwords in the **Trusted Users** database to use a trusted AP as a relay between the RADIUS server and the wireless clients. The wireless clients can then be authenticated by the RADIUS server.

8.4 Configuring Trusted AP

To configure trusted AP's on the ZyAIR's internal RADIUS, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted AP** tab. The screen appears as shown.

Figure 46 Trusted AP Screen

#	Active	IP Address	Shared Secret
1	<input checked="" type="checkbox"/>	127.0.0.1	
2	<input type="checkbox"/>	0.0.0.0	
3	<input type="checkbox"/>	0.0.0.0	
4	<input type="checkbox"/>	0.0.0.0	
5	<input type="checkbox"/>	0.0.0.0	
6	<input type="checkbox"/>	0.0.0.0	
7	<input type="checkbox"/>	0.0.0.0	
8	<input type="checkbox"/>	0.0.0.0	
9	<input type="checkbox"/>	0.0.0.0	
10	<input type="checkbox"/>	0.0.0.0	
30	<input type="checkbox"/>	0.0.0.0	
31	<input type="checkbox"/>	0.0.0.0	
32	<input type="checkbox"/>	0.0.0.0	

Apply Reset

The following table describes the labels in this screen.

Table 34 Trusted AP

LABEL	DESCRIPTION
#	This field displays the trusted AP index number.
Active	Select this checkbox to have the ZyAIR use the IP Address and Shared Secret to authenticate a trusted AP.
IP Address	Type the IP network address of the trusted AP in dotted decimal notation.

Table 34 Trusted AP

LABEL	DESCRIPTION
Shared Secret	Enter a password (up to 31 alphanumeric characters, no spaces) to be shared between the trusted AP and the ZyAIR. Note: The first trusted AP fields are reserved for the ZyAIR. They are grayed out and therefore cannot be configured. The shared secret must be the same on the trusted AP and your ZyAIR. The shared secret is not sent over the network. The shared secret is used to encrypt messages from and to the ZyAIR. Both the IP address and shared secret of the trusted AP can be configured in the "external RADIUS" server fields of the trusted AP.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

8.5 Trusted Users Overview

A trusted user is a wireless client within the ZyAIR's wireless network.

8.6 Configuring Trusted Users

To change your ZyAIR's trusted users, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted Users** tab. The screen appears as shown.

Figure 47 Trusted Users Screen

#	Active	User Name	Password
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
...			
31	<input type="checkbox"/>		
32	<input type="checkbox"/>		

Note. Password: Maximum 14 ASCII characters with PEAP

Apply Reset

The following table describes the labels in this screen.

Table 35 Trusted Users

LABEL	DESCRIPTION
#	This field displays the trusted user index number.
Active	Select this checkbox to have the ZyAIR authenticate wireless clients with the same user name and password activated on thier wireless utility.
User Name	Enter the username for this user account. This name can be up to 31 alphanumeric characters long, including spaces. The login name on the wireless client's utility must be the same as this user name on so it can authenticate the RADIUS server using the certificate information.
Password	Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. The password on the wireless client's utility must be the same as this password on so it can authenticate the RADIUS server using the certificate information. Note: If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.

Table 35 Trusted Users

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 9

WAN

This chapter describes how to configure WAN settings.

9.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

See the Wizard Setup chapter for more background information on most fields in the WAN screens. Background information on WAN fields not included in the Wizard is described here.

9.2 Configuring WAN ISP

To change your ZyAIR's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

9.2.1 Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

Figure 48 Ethernet Encapsulation

WAN

ISP IP MAC

ISP Parameters for Internet Access

Encapsulation Ethernet

Service Type Standard

Apply Reset

The following table describes the labels in this screen.

Table 36 Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from Standard , Telstra (RoadRunner Telstra authentication method), RR-Manager (Roadrunner Manager authentication method), RR-Toshiba (Roadrunner Toshiba authentication method) or Telia Login . The following fields do not appear with the Standard service type.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

9.2.1.1 Service Type

The screen varies according to the service type you select.

You need a username and password if your ISP is Time Warner's Roadrunner.

Figure 49 Ethernet Encapsulation

The following table describes the labels in this screen.

Table 37 Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from Standard , Telstra (RoadRunner Telstra authentication method), RR-Manager (Roadrunner Manager authentication method), RR-Toshiba (Roadrunner Toshiba authentication method) or Telia Login . The following fields do not appear with the Standard service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retye to Confirm	Type the password again to make sure that you have entered it correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server	This field only applies when you select Telia Login in the Service Type field. Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Every(min)	This field only applies when you select Telia Login in the Service Type field. The Telia server logs the ZyAIR out if the ZyAIR does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyAIR to wait between logins.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

9.2.2 PPPoE Encapsulation

The ZyAIR supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyAIR (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyAIR does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

Figure 50 PPPoE Encapsulation

WAN

ISP

IP

MAC

ISP Parameters for Internet Access

Encapsulation

PPP over Ethernet

Service Name

(optional)

User Name

Password

XXXXXXXXXX

Retype to Confirm

XXXXXXXXXX

☐ Nailed-Up Connection

Idle Timeout

100

(in seconds)

Apply

Reset

The following table describes the labels in this screen.

Table 38 PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPP over Ethernet choice is for a dial-up connection using PPPoE. The ZyAIR supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

9.2.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The screen shown next is for **PPTP** encapsulation.

Figure 51 PPTP Encapsulation

WAN

ISP IP MAC

ISP Parameters for Internet Access

Encapsulation: PPTP

User Name: [text field]

Password: [text field]

Retype to Confirm: [text field]

☐ Nailed-Up Connection

Idle Timeout: 100 (in seconds)

PPTP Configuration

☐ Get automatically from ISP (Default)

☒ Use fixed IP address

My IP Address: 0.0.0.0

My IP Subnet Mask: 0.0.0.0

Server IP Address: 0.0.0.0

Connection ID/Name: [text field]

Apply Reset

The following table describes the labels in this screen.

Table 39 PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyAIR supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyAIR automatically disconnects from the PPTP server.

Table 39 PPTP Encapsulation

LABEL	DESCRIPTION
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

9.3 TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

9.4 Configuring WAN IP

To change your ZyAIR's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**; otherwise click **Use fixed IP Address** and enter the IP address in the field provided.

Figure 52 WAN: IP

WAN

ISP IP **MAC**

WAN IP Address Assignment

☒ Get automatically from ISP (Default)
☐ Use fixed IP address

My WAN IP Address: 0.0.0.0
 Remote IP Address: 0.0.0.0
 Remote IP Subnet Mask: 0.0.0.0

Network Address Translation: SUA Only

Metric: 1
 Max NAT/Firewall Session Per User: 2048
 Private: No
 RIP Direction: None
 RIP Version: RIP-1
 Multicast: None

Windows Networking (NetBIOS over TCP/IP)

☒ Allow between LAN and WAN (You also need to create a firewall rule!)
☐ Allow Trigger Dial

Apply Reset

The following table describes the labels in this screen.

Table 40 WAN: IP

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
My WAN IP Subnet Mask (Ethernet only)	Type your network's IP subnet Mask.
Remote IP Address	Enter the Remote IP Address (if your ISP gave you one) in this field.
Gateway/Remote IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected Use Fixed IP Address .

Table 40 WAN: IP

LABEL	DESCRIPTION
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose None to disable NAT.</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p> <p>Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many- One-to-One and Server. When you select Full Feature you must configure at least one address mapping set!</p> <p>For more information about NAT refer to the <i>NAT</i> chapter in this <i>User's Guide</i>.</p>
Metric (PPPoE and PPTP only)	<p>This field sets this route's priority among the routes the ZyAIR uses.</p> <p>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".</p>
Max NAT/Firewall Session Per User	<p>Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.</p>
Private (PPPoE and PPTP only)	<p>This parameter determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.</p>
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets.</p> <p>Choose Both, None, In Only or Out Only.</p> <p>When set to Both or Out Only, the ZyAIR will broadcast its routing table periodically.</p> <p>When set to Both or In Only, the ZyAIR will incorporate RIP information that it receives.</p> <p>When set to None, the ZyAIR will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, RIP Direction is set to Both.</p>
RIP Version	<p>The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyAIR sends (it recognizes both formats when receiving). Choose RIP-1, RIP-2B or RIP-2M.</p> <p>RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the RIP Version field is set to RIP-1.</p>

Table 40 WAN: IP

LABEL	DESCRIPTION
Multicast	Choose None (default), IGMP-V1 or IGMP-V2 . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between WAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

9.5 Configuring WAN MAC

To change your ZyAIR's WAN MAC settings, click **WAN**, then the **WAN MAC** tab. The screen appears as shown.

Figure 53 MAC Setup

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.

CHAPTER 10

Single User Account (SUA) / Network Address Translation (NAT)

This chapter discusses how to configure SUA/NAT on the ZyAIR.

10.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

10.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyAIR. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 41 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.



Note: NAT never changes the IP address (either local or global) of an outside host.

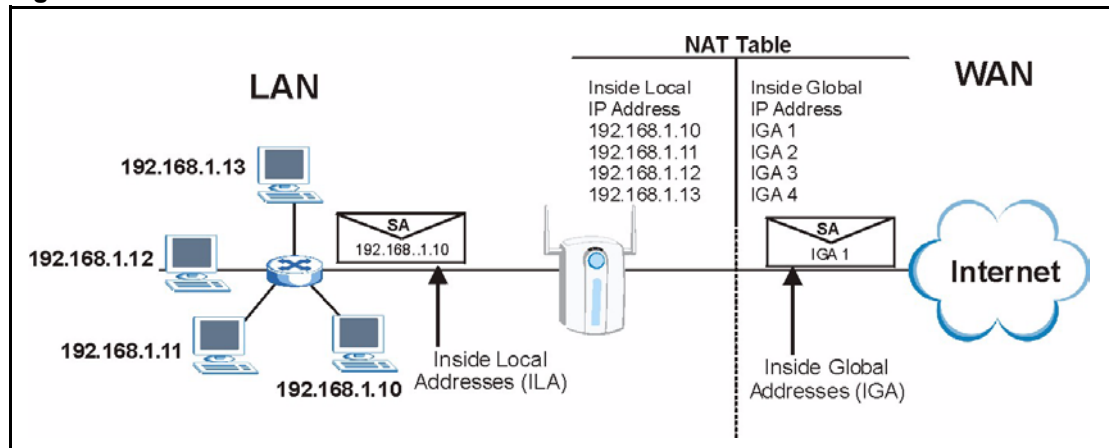
10.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyAIR filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

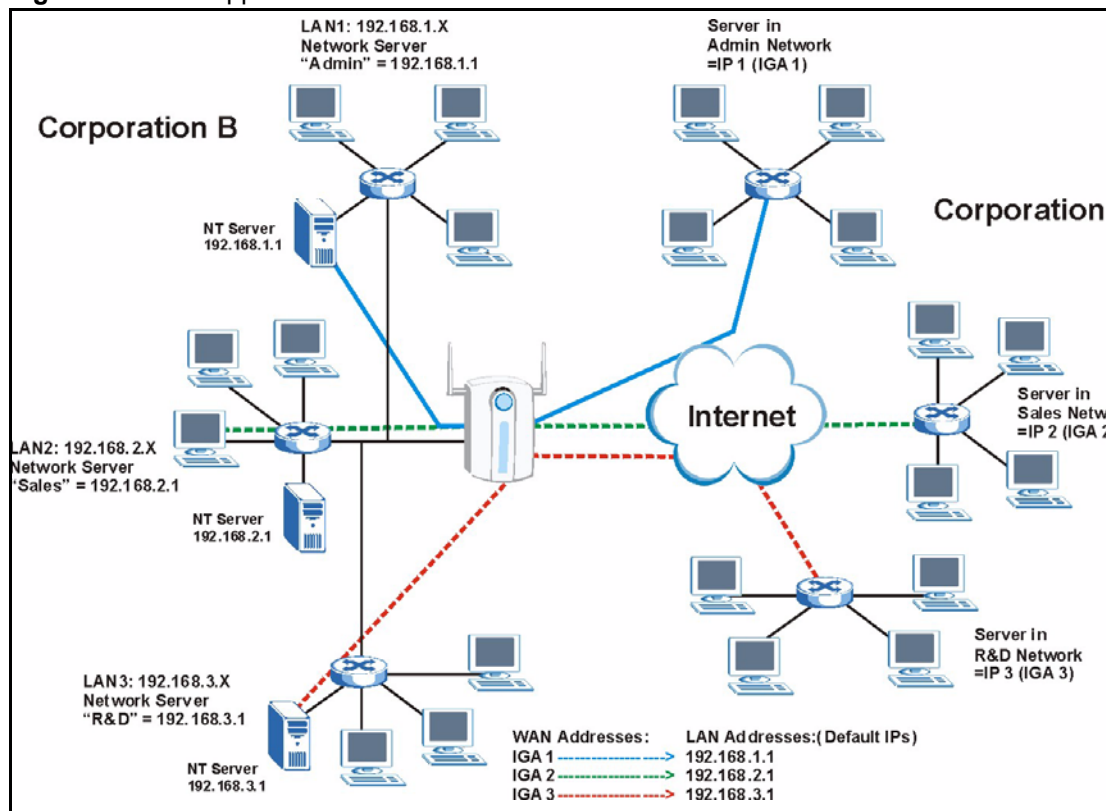
10.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyAIR keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 54 How NAT Works

10.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyAIR can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 55 NAT Application With IP Alias

10.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the ZyAIR maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the ZyAIR maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).
- **Many-to-Many Overload:** In Many-to-Many Overload mode, the ZyAIR maps the multiple local IP addresses to shared global IP addresses.
- **Many One-to-One:** In Many-One-to-One mode, the ZyAIR maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.



Note: Port numbers do not change for One-to-One and Many One-to-One NAT mapping types.

The following table summarizes these types.

Table 42 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1 \leftrightarrow IGA1	1-1
Many-to-One (SUA/PAT)	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA1 ...	M-1
Many-to-Many Overload	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA1 ILA4 \leftrightarrow IGA2 ...	M-M Ov
Many One-to-One	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA3 ...	M-1-1
Server	Server 1 IP \leftrightarrow IGA1 Server 2 IP \leftrightarrow IGA1 Server 3 IP \leftrightarrow IGA1	Server

10.2 Using NAT



Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyAIR.

10.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyAIR also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in the **WAN IP** screen.

10.3 SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

10.3.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen



Note: If you do not assign a Default Server IP Address, the ZyAIR discards all packets received for ports that are not specified in this screen or remote management.

10.3.2 Port Forwarding: Services and Port Numbers

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **SUA Server** page to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.



Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

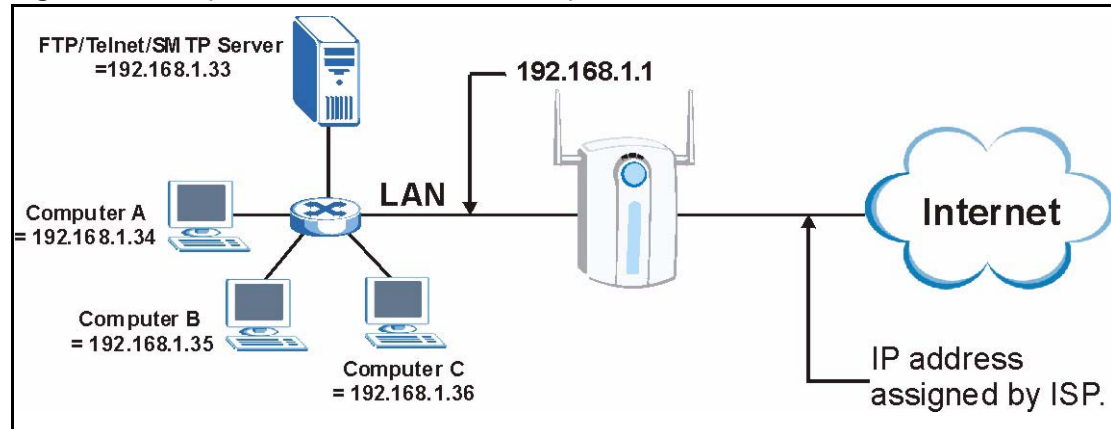
The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

Table 43 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

10.3.3 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet

Figure 56 Multiple Servers Behind NAT Example

10.4 Configuring SUA Server



Note: If you do not assign a Default Server IP Address, the ZyAIR discards all packets received for ports that are not specified in this screen or remote management.

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to [Figure 43](#) for port numbers commonly used for particular services.

Figure 57 SUA/NAT Setup

SUA/NAT

SUA Server **Addr Mapping** **Trigger Port**

Default Server: 0.0.0.0

#	Active	Name	Start Port	End Port	Server IP Address
1	<input type="checkbox"/>		0	0	0.0.0.0
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0

Apply Reset

The following table describes the labels in this screen.

Table 44 SUA/NAT Setup

LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a Default Server IP Address, the ZyAIR discards all packets received for ports that are not specified in this screen or remote management.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number here. To forward only one port, enter it again in the End Port field. To specify a range of ports, enter the last port to be forwarded in the End Port field.
End Port	
Server IP Address	Enter the inside IP address of the server here.

Table 44 SUA/NAT Setup

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

10.5 Configuring Address Mapping

Ordering your rules is important because the ZyAIR applies the rules in the order that you specify. When a rule matches the current packet, the ZyAIR takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyAIR's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.

Figure 58 Address Mapping

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

The following table describes the labels in this screen.

Table 45 Address Mapping

LABEL	DESCRIPTION
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address. Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with Many-to-One and Server mapping types.
Global End IP	This is the end Inside Global Address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Type	<ol style="list-style-type: none"> One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. Many One-to-One mode maps each local IP address to unique global IP addresses. Server allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Table 45 Address Mapping

LABEL	DESCRIPTION
Edit	Click Edit to go to the Address Mapping Rule screen.
Delete	Click Delete to delete an address mapping rule.

10.5.1 Configuring Address Mapping

To edit an address mapping rule, select the radio button of a rule and click the **Edit** button to display the screen shown next.

Figure 59 Address Mapping Edit

SUA/NAT

Address Mapping Rule

Type: One-to-One

Local Start IP: 0.0.0.0

Local End IP: N/A

Global Start IP: 0.0.0.0

Global End IP: N/A

Apply Cancel

The following table describes the labels in this screen.

Table 46 Address Mapping Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. 1. One-to-One : One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. Many-to-One : Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. Many-to-Many Overload : Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. Many One-to-One : Many One-to-one mode maps each local IP address to unique global IP addresses. 5. Server : This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping.

Table 46 Address Mapping Edit

LABEL	DESCRIPTION
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Apply	Click Apply to save your changes back to the ZyAIR.
Cancel	Click Cancel to return to the previous screen and not save your changes.

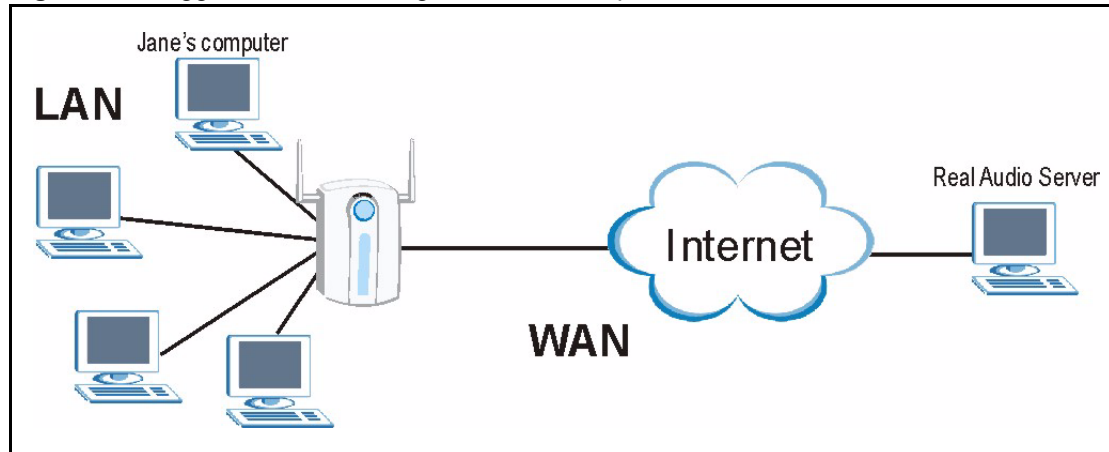
10.6 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyAIR records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyAIR's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyAIR forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

10.6.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 60 Trigger Port Forwarding Process: Example

- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a “trigger” port and causes the ZyAIR to record Jane’s computer IP address. The ZyAIR associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The ZyAIR forwards the traffic to Jane’s computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyAIR times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

10.6.2 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the ZyAIR and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

10.7 Configuring Trigger Port Forwarding

To change your ZyAIR’s trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.



Note: Only one LAN computer can use a trigger port (range) at a time

Figure 61 Trigger Port

SUA/NAT

SUA Server Addr Mapping Trigger Port

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

Apply Reset

The following table describes the labels in this screen.

Table 47 Trigger Port

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyAIR forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyAIR to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 11

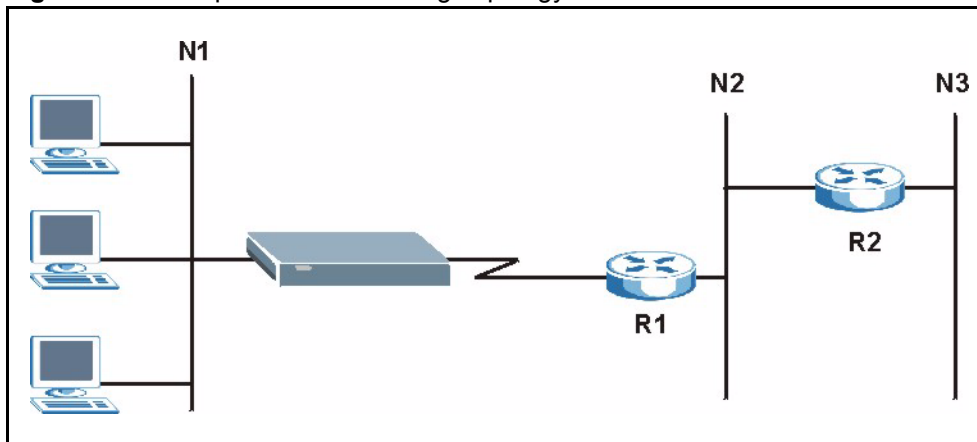
Static Route Screens

This chapter shows you how to configure static routes for your ZyAIR.

11.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyAIR has no knowledge of the networks beyond. For instance, the ZyAIR knows about network N2 in the following figure through remote node router R1. However, the ZyAIR is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node router R1 (via gateway router R2). The static routes are for you to tell the ZyAIR about the networks beyond the remote nodes.

Figure 62 Example of Static Routing Topology



11.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the screen as shown next.

Figure 63 Static Route

#	Name	Active	Destination	Gateway
1	-	-
2	-	-
3	-	-
4	-	-
5	-	-
6	-	-
7	-	-
8	-	-

The following table describes the labels in this screen.

Table 48 Static Route

LABEL	DESCRIPTION
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active (Yes) or not (No).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over the WAN, the gateway must be the IP address of one of the remote nodes.
Edit	Select a static route index number and then click Edit to set up a static route on the ZyAIR.
Delete	To remove a static route on the ZyAIR, click the radio button next to the static route index number you want to remove, then click Delete .

11.2.1 Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

Figure 64 Static Route: Edit

STATIC ROUTE - EDIT

Route Name

☐ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

☐ Private

The following table describes the labels in this screen.

Table 49 Static Route: Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyAIR will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Apply	Click Apply to save your changes back to the ZyAIR.
Cancel	Click Cancel to return to the previous screen and not save your changes.

CHAPTER 12

Remote Management Screens

This chapter provides information on the Remote Management screens.

12.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyAIR interface (if any) from which computers.



Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules

You may manage your ZyAIR from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable).



Note: When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The ZyAIR automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Console port
- 2 Telnet
- 3 HTTP

12.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
- 4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- 5 There is a firewall rule that blocks it.

12.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyAIR's WAN IP address when configuring from the WAN.
- Use the ZyAIR's LAN IP address when configuring from the LAN.

12.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyAIR automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

12.2 Configuring WWW

To change your ZyAIR's World Wide Web settings, click **REMOTE MGMT** to display the **WWW** screen.

Figure 65 Remote Management: WWW

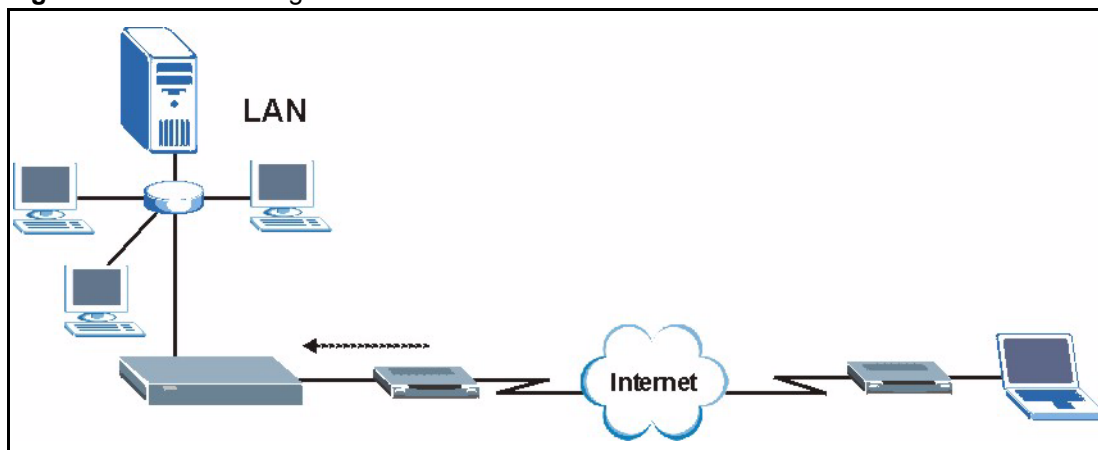
The following table describes the labels in this screen.

Table 50 Remote Management: WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.3 Configuring Telnet

You can configure your ZyAIR for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the ZyAIR.

Figure 66 Telnet Configuration on a TCP/IP Network

12.4 Configuring TELNET

Click **REMOTE MGMT** and the **TELNET** tab to display the screen as shown.

Figure 67 Remote Management: Telnet

The following table describes the labels in this screen.

Table 51 Remote Management: Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.

Table 51 Remote Management: Telnet

LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.5 Configuring FTP

You can upload and download the ZyAIR’s firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyAIR’s FTP settings, click **REMOTE MGMT**, then the **FTP** tab. The screen appears as shown.

Figure 68 Remote Management: FTP

The following table describes the labels in this screen.

Table 52 Remote Management: FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.

Table 52 Remote Management: FTP

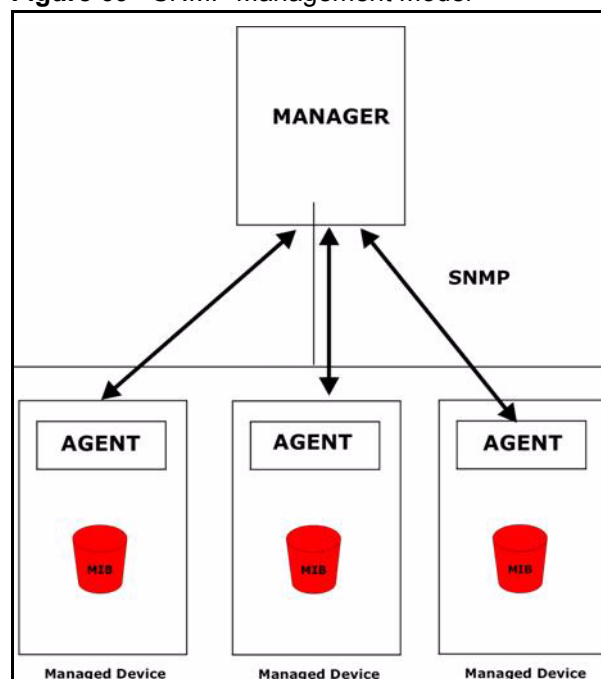
LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.



Note: SNMP is only available if TCP/IP is configured.

Figure 69 SNMP Management Model

An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyAIR). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

12.6.1 Supported MIBs

The ZyAIR supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

12.6.2 SNMP Traps

The ZyAIR will send traps to the SNMP manager when any one of the following events occurs:

Table 53 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).

Table 53 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

12.6.3 Configuring SNMP

To change your ZyAIR's SNMP settings, click **REMOTE MGMT**, then the **SNMP** tab. The screen appears as shown.

Figure 70 Remote Management: SNMP

REMOTE MANAGEMENT

TELNET FTP WWW **SNMP** DNS Security

SNMP Configuration

Get Community: public

Set Community: public

Trap Community: public

Destination: 0.0.0.0

SNMP

Service Port: 161

Service Access: LAN

Secured Client IP Address: ☒ All ☒ Selected 0.0.0.0

Apply Reset

The following table describes the labels in this screen.

Table 54 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trusted Host	If you enter a trusted host, your ZyAIR will only respond to SNMP messages from this address. A blank (default) field means your ZyAIR will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 54 Remote Management: SNMP

LABEL	DESCRIPTION
Service Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on Wizard Setup for background information.

To change your ZyAIR’s DNS settings, click **REMOTE MGMT**, then the **DNS** tab. The screen appears as shown.

Figure 71 Remote Management: DNS

The following table describes the labels in this screen.

Table 55 Remote Management: DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the ZyAIR.

Table 55 Remote Management: DNS

LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the ZyAIR. Select All to allow any computer to send DNS queries to the ZyAIR. Choose Selected to just allow the computer with the IP address that you specify to send DNS queries to the ZyAIR.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.8 Configuring Security

To change your ZyAIR's security settings, click **REMOTE MGMT**, then the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyAIR, an ICMP response packet is automatically returned. This allows the outside user to know the ZyAIR exists. Your ZyAIR supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyAIR when unsupported ports are probed.

Figure 72 Security

The following table describes the labels in this screen.

Table 56 Security

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyAIR will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN & WAN to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyAIR by probing for unused ports. If you select this option, the ZyAIR will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyAIR unseen. By default this option is not selected and the ZyAIR will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyAIR's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyAIR reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcp rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 13

UPnP

This chapter introduces the Universal Plug and Play feature.

13.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

13.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

13.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- 1 Dynamic port mapping
- 2 Learning public IP addresses
- 3 Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the *SUA/NAT* chapter for further information about NAT.

13.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

13.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

Please see later in this *User's Guide* for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

13.3 Configuring UPnP

Click **UPnP** to display the screen shown next.

Figure 73 Configuring UPnP

UPnP

Device Name: ZyXEL ZyAIR G-2000PLUS Internet Sharing Gateway

☐ Enable the Universal Plug and Play (UPnP) Feature

☐ Allow users to make configuration changes through UPnP

☐ Allow UPnP to pass through Firewall

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

Apply Reset

The following table describes the labels in this screen.

Table 57 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyAIR's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyAIR so that they can communicate through the ZyAIR, for example by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

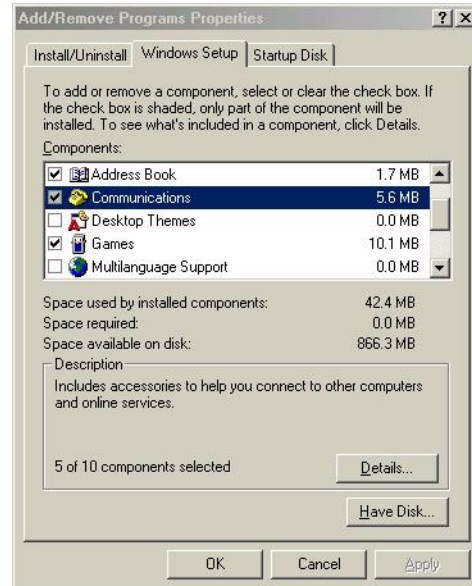
13.4 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

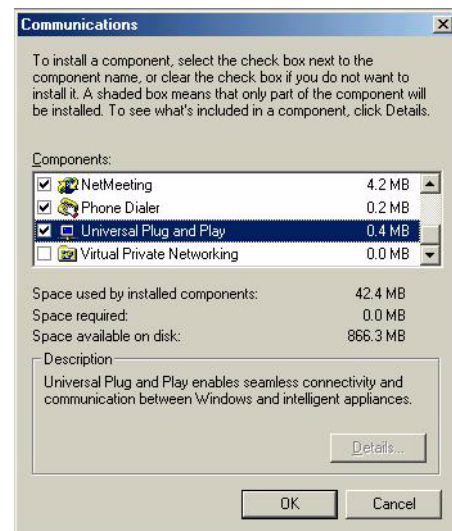
13.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



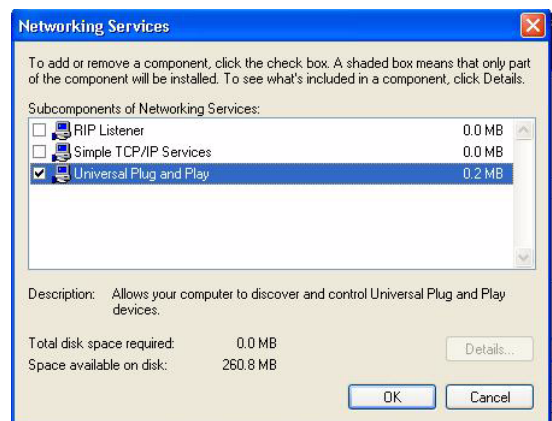
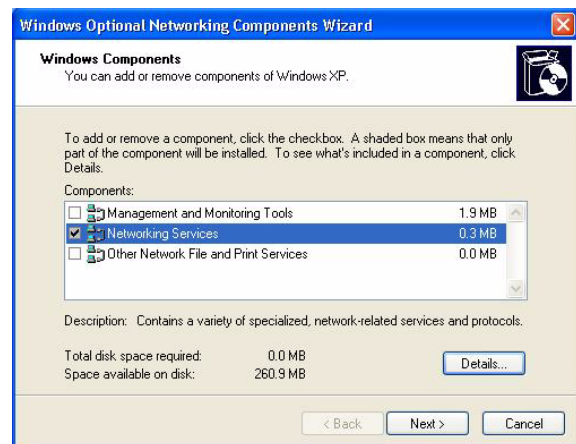
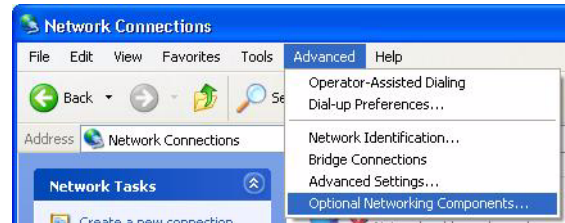
- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.



13.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components**
- 4 The **Windows Optional Networking Components Wizard** window displays.
- 5 Select **Networking Service** in the **Components** selection box and click **Details**.
- 6 In the **Networking Services** window, select the **Universal Plug and Play** check box.
- 7 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



13.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

13.5.1 Auto-discover Your UPnP-enabled Network Device

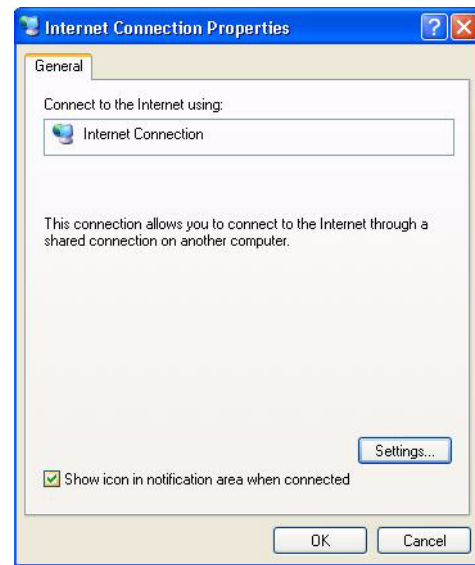
- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.



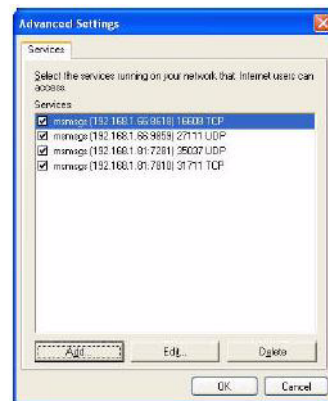
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.
- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 5** Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



- 6** Double-click the icon to display your current Internet connection status.

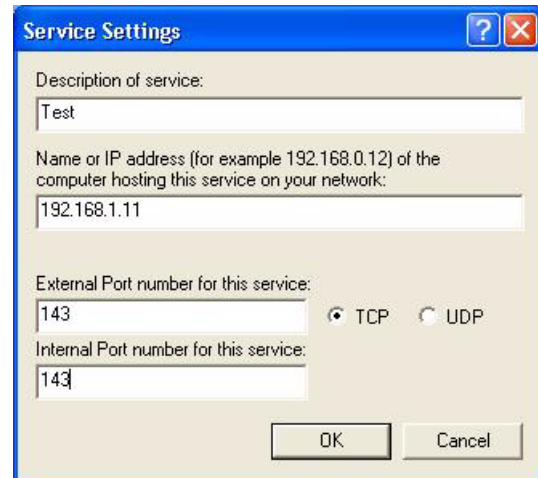


13.5.2 Web Configurator Easy Access

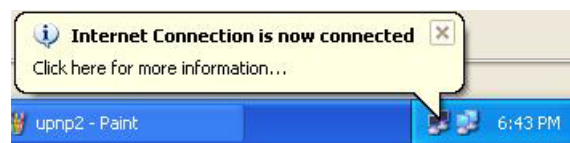
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.
- 6 Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.

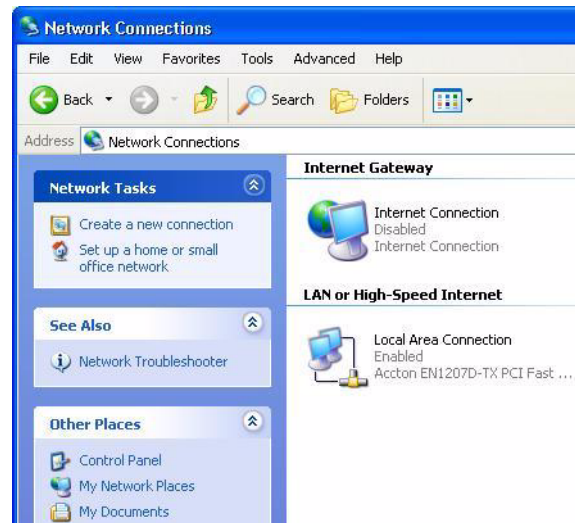


13.5.3 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

- 1 Click Start and then Control Panel.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.
- 6 Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.



CHAPTER 14

Firewalls

This chapter gives some background information on firewalls and introduces the ZyAIRZyAIR firewall.

14.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

14.2 Types of Firewalls

There are three main types of firewalls:

- 1 Packet Filtering Firewalls
- 2 Application-level Firewalls
- 3 Stateful Inspection Firewalls

14.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

14.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

- 1 Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.
- 2 Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

14.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. See "Stateful Inspection" on page 185 for more information on Stateful Inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

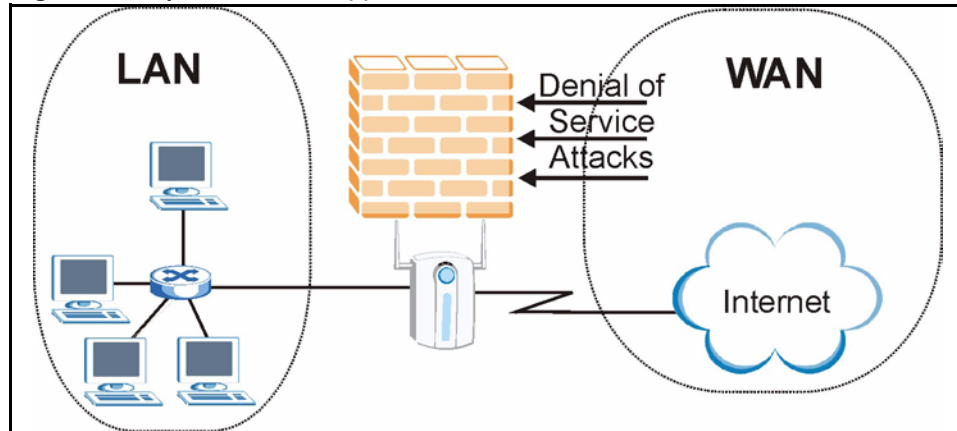
14.3 Introduction to ZyXEL's Firewall

The ZyAIR firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The ZyAIR's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyAIR can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyAIR also has packet-filtering capabilities.

The ZyAIR is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyAIR has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into two areas.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, inbound access will not be allowed unless the remote host is authorized to use a specific service.

Figure 74 ZyAIR Firewall Application

14.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyAIR is pre-configured to automatically detect and thwart all known DoS attacks.

14.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An extension number, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

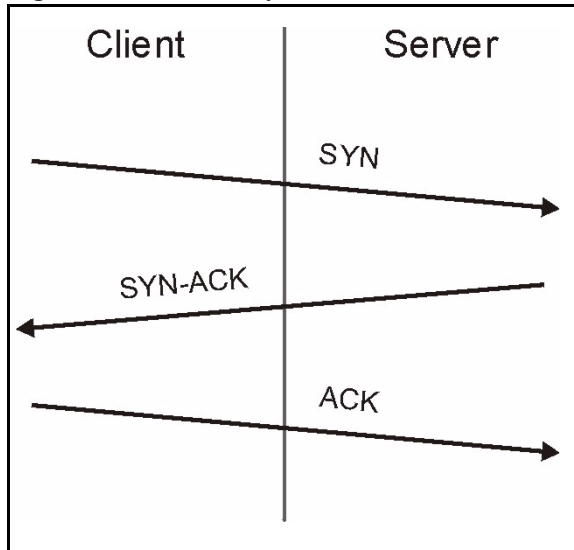
Table 58 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

14.4.2 Types of DoS Attacks

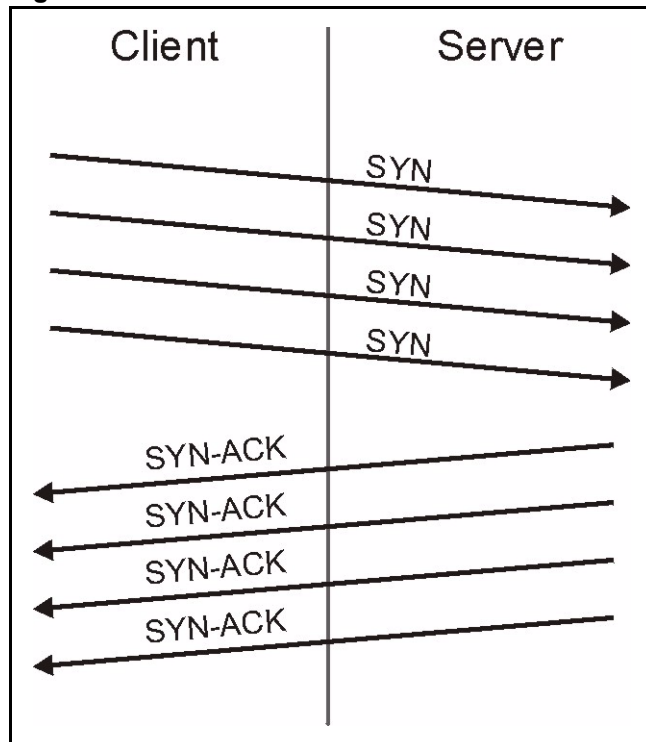
There are four types of DoS attacks:

- 1 Those that exploit bugs in a TCP/IP implementation.
 - 2 Those that exploit weaknesses in the TCP/IP specification.
 - 3 Brute-force attacks that flood a network with useless data.
 - 4 IP Spoofing.
- **"Ping of Death"** and **"Teardrop"** attacks exploit bugs in the TCP/IP implementations of various computer and host systems.
 - a Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
 - b Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.
 - Weaknesses in the TCP/IP specification leave it open to **"SYN Flood"** and **"LAND"** attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

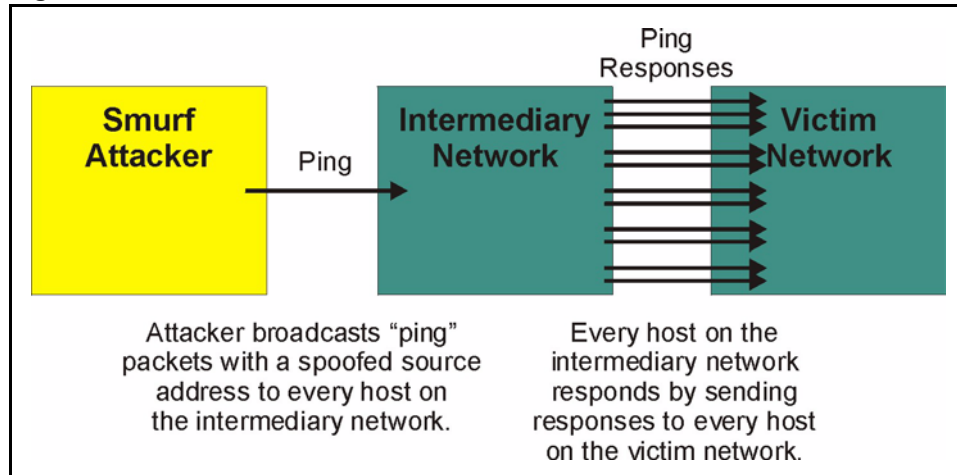
Figure 75 Three-Way Handshake

Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

- a SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

Figure 76 SYN Flood

- b** In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.
- A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 77 Smurf Attack

14.4.2.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 59 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

14.4.2.2 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

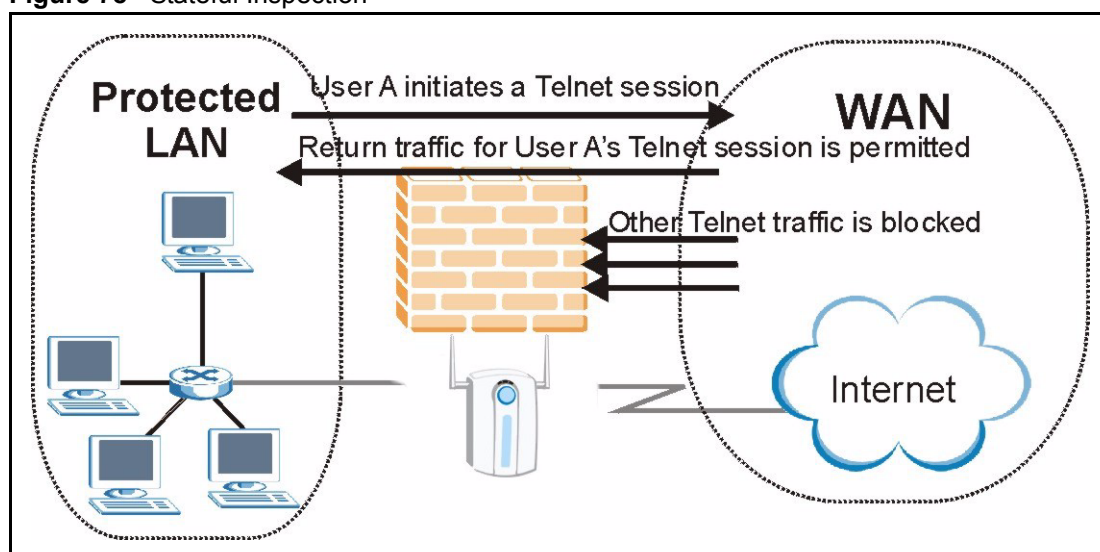
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyAIR blocks all IP Spoofing attempts.

14.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This remembering is called *saving the state*. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyAIR uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyAIR's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 78 Stateful Inspection



The previous figure shows the ZyAIR's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

14.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

- 1 The packet travels from the firewall's LAN to the WAN.
- 2 The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).

- 3 The firewall inspects packets to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then the setting in the **Firewall Default Rule** screen determines the action for this packet.
- 4 Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
- 5 The outbound packet is forwarded out through the interface.
- 6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
- 7 The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

14.5.2 Stateful Inspection and the ZyAIR

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- 1 Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- 2 Allow certain types of traffic from the Internet to specific hosts on the LAN.
- 3 Allow access to a Web server to everyone but competitors.
- 4 Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.



Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyAIR itself (as with the "virtual connections" created for UDP and ICMP).

14.5.3 TCP Security

The ZyAIR uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyAIR receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

14.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyAIR is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

14.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyAIR inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's **Custom Services** feature to do this.

14.6 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via SMT or web configurator.
- 2 Think about access control before you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
- 3 Limit who can telnet into your router.
- 4 Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

14.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyAIR's filtering and firewall functions.

14.7.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

14.7.1.1 When To Use Filtering

- 1 To block/allow LAN packets by their MAC addresses.
- 2 To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- 3 To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4 To block/allow IP trace route.

14.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

14.7.2.1 When To Use The Firewall

- 1 To prevent DoS attacks and prevent hackers cracking your network.
- 2 A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
- 3 To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4 The firewall performs better than filtering if you need to check many rules.
- 5 Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.

- 6** The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

CHAPTER 15

Firewall Screens

This chapter shows you how to configure your ZyAIR firewall.

15.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyAIR has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to the *Appendix* for firewall CLI commands.

15.2 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ZyAIR
- LAN to WAN
- WAN to LAN
- WAN to WAN/ZyAIR



Note: The LAN includes both the LAN port and the WLAN.

By default, the ZyAIR's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ZyAIR

This allows computers on the LAN to manage the ZyAIR and communicate between networks or subnets connected to the LAN interface.

- LAN to WAN

By default, the ZyAIR's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ZyAIR

This prevents computers on the WAN from using the ZyAIR as a gateway to communicate with other computers on the WAN and/or managing the ZyAIR.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.



Note: If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyAIR's default rules.

15.3 Rule Logic Overview



Note: Study these points carefully before configuring rules.

15.3.1 Rule Checklist

- 1 State the intent of the rule. For example, This restricts all IRC access from the LAN to the Internet. Or, This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.
- 2 Is the intent of the rule to forward or block traffic?
- 3 What direction of traffic does the rule apply to (See “Types of Firewalls” on page 178)?
- 4 What IP services will be affected?
- 5 What computers on the LAN are to be affected (if any)?
- 6 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

15.3.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

- 1** Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2** Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3** Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4** Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

15.3.3 Key Fields For Configuring Rules

15.3.3.1 Action

Should the action be to **Block** or **Forward**?



Note: “Block” means the firewall silently discards the packet.

15.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See “Predefined Services” on page 206 for more information on predefined services.

15.3.3.3 Source Address

What is the connection’s source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

15.3.3.4 Destination Address

What is the connection’s destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

15.4 Connection Direction Examples

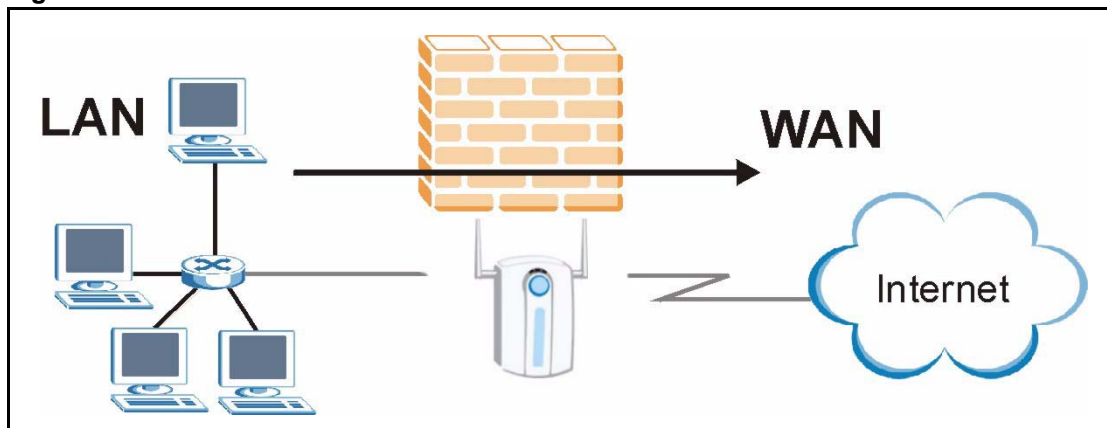
This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ZyAIR and WAN to WAN/ZyAIR rules apply to packets coming in on the associated interface (LAN or WAN respectively). LAN to LAN/ZyAIR means policies for LAN-to-ZyAIR (the policies for managing the ZyAIR through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/ZyAIR policies apply in the same way to the WAN ports.

15.4.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

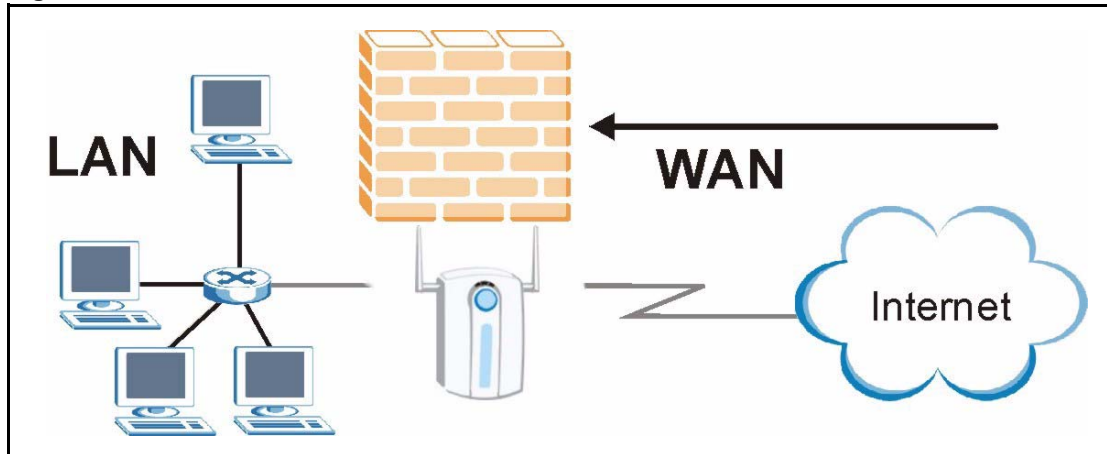
Figure 79 LAN to WAN Traffic



15.4.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

See the following figure.

Figure 80 WAN to LAN Traffic

15.5 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when a rule is matched in the **Edit Rule** screen ([Figure 83](#)). Configure the **Log Settings** screen to have the ZyAIR send an immediate e-mail message to you when an event generates an alert. Refer to the chapter on logs for details.

15.6 Configuring Firewall

Click **FIREWALL** to open the **Default Rule** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in the following screen.

Figure 81 Default Rule

FIREWALL

Default Rule Rule Summary

☒ Enable Firewall

☐ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN and WAN to WAN packets will bypass the Firewall check.)

Packet Direction	Default Action	Log
(W)LAN to (W)LAN / ZyAIR	Forward	<input type="checkbox"/>
(W)LAN to WAN	Forward	<input type="checkbox"/>
WAN to WAN / ZyAIR	Block	<input type="checkbox"/>
WAN to (W)LAN	Block	<input checked="" type="checkbox"/>

Apply Reset

The following table describes the labels in this screen.

Table 60 Default Rule

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyAIR performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Allow Asymmetrical Route	Select this check box to have the ZyAIR firewall permit the use of triangle route topology on the network. See the <i>Appendix</i> for more on triangle route topology.
Packet Direction	This is the direction of travel of packets ((W)LAN to (W)LAN/ZyAIR, (W)LAN to WAN, WAN to (W)LAN, WAN to WAN/ZyAIR). Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, (W)LAN to (W)LAN/ZyAIR means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyAIR or the ZyAIR itself.
Default Action	Use the drop-down list boxes to select whether to Block (silently discard) or Forward (allow the passage of) packets that are traveling in the selected direction.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

15.6.1 Rule Summary



Note: The ordering of your rules is very important as rules are applied in turn.

Click **FIREWALL**, then the **Rule Summary** tab to open the screen.

Figure 82 Rule Summary

FIREWALL

Default Rule Rule Summary

Firewall Rules Storage Space in Use

0% 2% 100%

Packet Direction (W)LAN to (W)LAN / ZyAIR

Default Policy: Forward, None Log

#	Active	Source Address	Destination Address	Service Type	Action	Schedule	Log	Alert
---	--------	----------------	---------------------	--------------	--------	----------	-----	-------

Move rule 1 to rule 1 (rule number).

Edit Create Delete

The following table describes the labels in this screen.

Table 61 Rule Summary

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyAIR's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets ((W)LAN to (W)LAN/ZyAIR, (W)LAN to WAN, WAN to (W)LAN, WAN to WAN/ZyAIR) for which you want to configure firewall rules.
Default Policy	This field displays the default action and log policy you selected in the Default Rule screen for the packet direction shown in the field above.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click + to expand or - to collapse the Source Address , Destination Address and Service Type drop down lists.
Active	This field displays whether a firewall is turned on (Y) or not (N).
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Service Type	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to Any . See Table 64 for more information.

Table 61 Rule Summary

LABEL	DESCRIPTION
Action	This is the specified action for that rule, either Block or Forward . Note that Block means the firewall silently discards the packet.
Schedule	This field tells you whether a schedule is specified (Yes) or not (No).
Log	This field shows you whether a log is created when packets match this rule (Enabled) or not (Disable).
Alert	This field tells you whether this rule generates an alert (Yes) or not (No) when the rule is matched.
Move	Type a rule's index number and the number for where you want to put that rule. Click Move to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. Type the index number for where you want to put a rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
Edit	Click Edit to go to the screen where you can edit the rule.
Create	Click Create to go to the screen where you can configure a new firewall rule.
Delete	Click Delete to delete an existing firewall rule. A window display asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.

15.6.2 Configuring Firewall Rules

Follow these directions to create a new rule.

- 1** In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
- 2** Click **Insert** to display this screen and refer to the following table for information on the labels.

Figure 83 Creating/Editing A Firewall Rule

FIREWALL

☒ **Active Rule**

Edit Source Address

Address Editor Address Type Any Address Start IP Addr. End IP Addr. Subnet Mask <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Add Modify </div>	Source Address(es) <div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">Any</div> <div style="text-align: right; margin-top: 5px;">Delete</div>
---	---

Edit Destination Address

Address Editor Address Type Any Address Start IP Addr. End IP Addr. Subnet Mask <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Add Modify </div>	Destination Address(es) <div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">Any</div> <div style="text-align: right; margin-top: 5px;">Delete</div>
---	--

Edit Service

Available Services : <div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"> AIM/NEW_ICQ(TCP:5190) AUTH(TCP:113) BGP(TCP:179) BOOTP_CLIENT(UDP:68) BOOTP_SERVER(UDP:67) </div>	<< >>	Selected Services : <div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"> Any(UDP) Any(TCP) </div>
--	--------------	---

Custom Service:

Add
Edit
Delete

Edit Schedule

Day to Apply:
☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Time of Day to Apply: (24-Hour Format)
☒ All day

Start(hh-mm) 00 : 00 End(hh-mm) 00 : 00

Actions When Matched

Log None

☐ Alert Message to Administrator When Matched

Action for Matched Packets Forward

Apply
Cancel

The following table describes the labels in this screen.

Table 62 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Edit Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: Single Address , Range Address , Subnet Address and Any Address .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add	Click Add to add a new address to the Source or Destination Address(es) box. You can add multiple addresses, ranges of addresses, and/or subnets.
Modify	To edit an existing source or destination address, select it from the box and click Modify .
Delete	Highlight an existing source or destination address from the Source or Destination Address(es) box above and click Delete to remove it.
Edit Service	
Available/ Selected Services	Please Table 64 for more information on services available. Highlight a service from the Available Services box on the left, then click >> to add it to the Selected Service(s) box on the right. To remove a service, highlight it in the Selected Service(s) box on the right, then click <<.
Custom Service	
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an *) from the Available Services list and click this button to edit the service.
Delete	Select a custom service (denoted by an *) from the Available Services list and click this button to remove the service.
Edit Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select All Day or enter the start and end times in the hour-minute format to apply the rule.
Actions When Matched	
Log	This field determines if a log is created or not for the following options. Select Match to create a log for packets that match the rule. If you do not want to create a log select None . Select Not-Match to create a log for packets that do not match the rule. Select Both to create a log for packets that match the rule and packets that do not match the rule. Go to the Log Settings page and select the Access Control logs category to have the ZyAIR record these logs.
Alert Message to Administrator When Matched	Select the check box to have the ZyAIR generate an alert when the rule is matched.

Table 62 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Action for Matched Packets	Use the drop-down list box to select whether to discard (Block) or allow the passage of (Forward) packets that match this rule.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

15.6.3 Configuring Custom Services

Configure customized ports for services not predefined by the ZyAIR (See “Predefined Services” on page 206 for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click the **Add** button under **Custom Service** while editing a firewall rule to configure a custom service. This displays the following screen.

Figure 84 Creating/Editing A Custom Service

The screenshot shows a web interface titled "FIREWALL" with a sub-section "Custom Service". It contains the following elements:

- Service Name:** A text input field.
- Service Type:** A dropdown menu currently showing "TCP/UDP".
- Service Port:** A section with two radio buttons: "Single" (selected) and "Range".
 - Under "Single": A text input field with "0".
 - Under "Range": Two text input fields labeled "From" and "To", both containing "0".
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

The following table describes the labels in this screen.

Table 63 Creating/Editing A Custom Service

LABEL	DESCRIPTION
Service Name	Enter a unique name for your custom service.
Service Type	Choose the IP port (TCP , UDP or Both) that defines your customized service from the drop down list box.
Port	Select Single to specify one port only or Range to specify a span of ports that define your customized service.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

15.7 Example Firewall Rule

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

- 1 Click the **FIREWALL** link and then the **Rule Summary** tab. Select **WAN to LAN** from the **Packet Direction** drop-down list box.

Figure 85 Rule Summary

FIREWALL

Default Rule Rule Summary

Firewall Rules Storage Space in Use
0% 15% 100%

Packet Direction: WAN to (W)LAN
Default Policy: Forward, Log

#	Active	Source Address	Destination Address	Service Type	Action	Schedule	Log	Alert
1	Y	Any	Any	Any(UDP)	Forward	No	None	Yes
2	Y	Any	Any	BOOTP_CLIENT(UDP:68)	Forward	Yes	Match	Yes

Move rule 1 to rule 1 (rule number).

Edit Create Delete

- 2 In the **Rule Summary** screen, type the index number for where you want to put the rule, assuming you have more than one rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
- 3 Click **Create** to display the firewall **Edit Rule** screen.
- 4 In the **Edit Rule** screen, select **Any** in the **Destination Address** box and then click **Delete**.
- 5 Configure the destination address screen as follows.

Figure 86 Rule Edit Example

FIREWALL

☒ Active Rule

Edit Source Address

Address Editor

Address Type: Any Address

Start IP Addr.:

End IP Addr.:

Subnet Mask:

Add Modify

Source Address(es): Any

Delete

Edit Destination Address

Address Editor

Address Type: Range Address

Start IP Addr.: 10.0.0.10

End IP Addr.: 10.0.0.15

Subnet Mask:

Add Modify

Destination Address(es): Any

Delete

- 6** In the **Edit Rule** screen, click **Add** under **Custom Service** to open the **Edit Custom Service** screen. Configure it as follows and click **Apply**.

Figure 87 Edit Custom Service Example

FIREWALL

Custom Service

Service Name: My Service

Service Type: TCP/UDP

Service Port: ☒ Single 123 ☐ Range From 0 To 0

Apply Cancel

- 7** In the **Edit Rule** screen, use the arrows between **Available Services** and **Selected Service(s)** to configure it as follows. Click **Apply** when you are done.



Note: Custom services show up with an * before their names in the **Services** list box and the **Rule Summary** list box. Click **Apply** after you've created your custom service.

Figure 88 My Service Rule Configuration

FIREWALL

☒ Active Rule

Edit Source Address

Address Editor

Address Type: Any Address

Start IP Addr.:

End IP Addr.:

Subnet Mask:

Add Modify

Source Address(es): Any

Delete

Edit Destination Address

Address Editor

Address Type: Any Address

Start IP Addr.:

End IP Addr.:

Subnet Mask:

Add Modify

Destination Address(es): 10.0.0.10 - 10.0.0.15

Delete

Edit Service

Available Services :

*Treat(TCP/UDP:53)
Any(TCP)
Any(UDP)
AIM/NEW_ICQ(TCP:5190)
AUTH(TCP:113)

<< >>

Selected Services :

*My Service(TCP/UDP:123)

Custom Service:

Add Edit Delete

Edit Schedule

Day to Apply:

☒ Sun ☒ Mon ☒ Tue ☐ Wed ☐ Thu ☒ Fri ☒ Sat

Time of Day to Apply: (24-Hour Format)

☐ All day

Start(hh-mm): 10 : 30 End(hh-mm): 11 : 30

Actions When Matched

Log: Match

☒ Alert Message to Administrator When Matched

Action for Matched Packets: Forward

Apply Cancel

Figure 89 My Service Example Rule Summary

FIREWALL

Default Rule Rule Summary

Firewall Rules Storage Space in Use

0% 15% 100%

Packet Direction: WAN to (W)LAN

Default Policy: Forward, Log

#	Active	Source Address	Destination Address	Service Type	Action	Schedule	Log	Alert
1	Y	Any	Any	Any(UDP)	Forward	No	None	Yes
2	Y	Any	10.0.0.10 - 10.0.0.15	*My Service(TCP/UDP:123)	Forward	Yes	Match	Yes

Move rule 1 to rule 1 (rule number).

Edit Create Delete

Rule 1: Allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

15.8 Predefined Services

The **Available Services** list box in the **Edit Rule** screen ([Figure 83](#)) displays all predefined services that the ZyAIR already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled **(DNS)**. **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Custom services may also be configured using the **Custom Services** function discussed previously.

Table 64 Predefined Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME (TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 64 Predefined Services (continued)

SERVICE	DESCRIPTION
FTP(TCP:20,21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TRANSPORT / TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger (TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NetBIOS(TCP/UDP:137~139, 45)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
ROADRUNNER(TCP/UDP:1026)	This is Time Warner's cable modem session management protocol. It handles authentication and dynamic addressing.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.

Table 64 Predefined Services (continued)

SERVICE	DESCRIPTION
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP(UDP:1900)	Simple Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using UDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

CHAPTER 16

Content Filtering

This chapter provides a brief overview of content filtering using the embedded WebGUI.

16.1 Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords and should not be confused with packet filtering via SMT menu 21.1. To access these functions, from the **Main Menu**, click **Content Filter** to expand the Content Filter menus.

16.2 Restrict Web Features

The ZyAIR can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

16.3 Days and Times

The ZyAIR also allows you to define time periods and days during which the ZyAIR performs content filtering.

16.4 Configure Content Filtering

Click **Content Filter** on the navigation panel, to open the following screen.

Figure 90 Content Filter

FIREWALL

Rule Summary

Restrict Web Features ☐ ActiveX ☐ Java ☒ Cookies ☐ Web Proxy

☒ Enable URL Keyword Blocking

Keyword

Keyword List

playboy

Add Delete Clear All

Denied Access Message Restricted Access

Day to Block

☐ Everyday ☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat

Time of Day to Block (24-Hour Format)

☒ All day

Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

Apply Reset

The following table describes the labels in this screen.

Table 65 Content Filter

LABEL	DESCRIPTION
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The ZyAIR can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.

Table 65 Content Filter

LABEL	DESCRIPTION
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click Add after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click Delete to remove it. The keyword disappears from the text box after you click Apply .
Clear All	Click this button to remove all of the listed keywords.
Day to Block	Select check boxes for the days that you want the ZyAIR to perform content filtering. Select the Everyday check box to have content filtering turned on all days of the week.
Time of Day to Block	Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Enter the time period, in 24-hour format, during which content filtering will be enforced. Select the All Day check box to have content filtering always active on the days selected in Day to Block with time of day limitations not enforced.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh

CHAPTER 17

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

17.1 Certificates Overview

The ZyAIR can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyAIR to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyAIR uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyAIR does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyAIR can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

17.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyAIR only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

17.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the ZyAIR act as a certification authority and sign its own certificates.

17.3 Configuration Summary

This section summarizes how to manage certificates on the ZyAIR.

Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyAIRs' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the ZyAIR.

17.4 My Certificates

Click **CERTIFICATES**, **My Certificates** to open the ZyAIR's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

Figure 91 My Certificates

CERTIFICATES

My Certificates **Trusted CAs**

PKI Storage Space in Use

0% 3% 100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyAIR models. Click Replace to create a certificate using your ZyAIR's MAC address that will be specific to this device.

My Certificates Setting

#	Name	Type	Subject	Issuer	Valid From	Valid To
1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-2000PLUS Factory Default Certificate	CN=ZyAIR G-2000PLUS Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

The following table describes the labels in this screen.

Table 66 My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyAIR's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyAIR has the factory default certificate. The factory default certificate is common to all ZyAIRs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyAIR's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 66 My Certificates (continued)

LABEL	DESCRIPTION
Type	<p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>*SELF represents the default self-signed certificate, which the ZyAIR uses to sign imported trusted remote host certificates.</p> <p>CERT represents a certificate issued by a certification authority.</p>
Subject	<p>This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.</p>
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.</p>
Valid From	<p>This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.</p>
Valid To	<p>This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.</p>
Details	<p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use.</p> <p>Do the following to delete a certificate that shows *SELF in the Type field.</p> <ol style="list-style-type: none"> 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the *SELF certificate. 2. Click the details icon next to another self-signed certificate (see the description on the Create button if you need to create a self-signed certificate). 3. Select the Default self-signed certificate which signs the imported remote host certificates check box. 4. Click Apply to save the changes and return to the My Certificates screen. 5. The certificate that originally showed *SELF displays SELF and you can delete it now. <p>Note that subsequent certificates move up by one when you take this action</p>
Create	<p>Click Create to go to the screen where you can have the ZyAIR generate a certificate or a certification request.</p>
Import	<p>Click Import to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyAIR.</p>
Delete	<p>Click Delete to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.</p>
Refresh	<p>Click Refresh to display the current validity status of the certificates.</p>

17.5 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyAIR currently allows the importation of a PKCS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

17.6 Importing a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyAIR, see the following figure.



Note: 1. You can only import a certificate that matches a corresponding certification request that was generated by the ZyAIR.

Note: 2. The certificate you import replaces the corresponding request in the My Certificates screen.

Note: 3. You must remove any spaces from the certificate's filename before you can import it.

Figure 92 My Certificate Import

The following table describes the labels in this screen.

Table 67 My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the ZyAIR.
Cancel	Click Cancel to quit and return to the My Certificates screen.

17.7 Creating a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyAIR create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

Figure 93 My Certificate Create

CERTIFICATES

Certificate Name

Subject Information

Common Name

- ☒ Host IP Address
- ☐ Host Domain Name
- ☐ E-Mail

Organizational Unit

Organization

Country

Key Length bits

Enrollment Options

☒ Create a self-signed certificate

☐ Create a certification request and save it locally for later manual enrollment

☐ Create a certification request and enroll for a certificate immediately online

Enrollment Protocol

CA Server Address

CA Certificate (See [Trusted CAs](#))

Request Authentication Reference Number

Key

Apply

Cancel

The following table describes the labels in this screen.

Table 68 My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the Common Name is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyAIR drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyAIR drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyAIR drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select Create a self-signed certificate to have the ZyAIR generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select Create a certification request and save it locally for later manual enrollment to have the ZyAIR generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the My Certificate Details screen (see the My Certificate Details section) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select Create a certification request and enroll for a certificate immediately online to have the ZyAIR generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the Trusted CAs screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.

Table 68 My Certificate Create (continued)

LABEL	DESCRIPTION
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the CA Certificate drop-down list box. You must have the certification authority's certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the ZyAIR's list of certificates of trusted certification authorities.
Request Authentication	When you select Create a certification request and enroll for a certificate immediately online , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just fill in the Key field if your certification authority uses the SECP enrollment protocol.
Key	Type the key that the certification authority gave you.
Apply	Click Apply to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyAIR is generating the self-signed certificate or certification request.

After the ZyAIR successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyAIR enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyAIR to enroll a certificate online.

17.8 My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see [Figure 91](#)). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyAIR uses to sign the trusted remote host certificates that you import to the ZyAIR.

Figure 94 My Certificate Details

CERTIFICATES

Name

Property
☒ Default self-signed certificate which signs the imported remote host certificates.

Certificate Path

Searching...

Certificate Information

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946684804
Subject	CN=ZyAIR G-2000PLUS Factory Default Certificate
Issuer	CN=ZyAIR G-2000PLUS Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=factory@auto.gen.cert
Key Usage Basic Constraint	DigitalSignature, KeyEncipherment, KeyCertSign Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	ae:96:ec:3c:31:5f:47:6a:a8:cd:cd:8d:e8:89:9a:9c
SHA1 Fingerprint	29:c5:8f:be:64:2d:1d:1f:4f:f5:20:d7:51:ad:86:e6:77:85:63:cc

Certificate in PEM (Base-64) Encoded Format

```

MIIBqjCCAVSgAwIBAgIEOG1DhDANBgkqhkiG9w0BAQUFADA3MTUwMwYDVQQDEyxaeU
FJU1BHLTIwMDBQTFVtIEZyY3RvcnkGRGVmYXVsdCBDZXJ0aWZpY2F0ZTAeFw0w
MDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBaMDcxNTAzBgNVBAMTLFp5QU1SIEct
MjAwMFBhVGVmRmFjdG9yeSBZw2hdWx0IENlcjZm1jYXR1MFwDQYJKoZIhvcN
AQEBBQADSwAwSABAKCg/9pDXhyWIEpJ3PV/ONdIbClz67qDE2p30zNNuz5SkH2
qetvotua1O+11f6xWA57YuR5twAGnV4EQoZsRuMCAwEAANIMEYwDgYDVROPAQEA
BAQDAgKkKCAgA1UdEQQZMBEwFwZyY3Rvcn1AYXV0by5nZW4uY2VydASBgNVHRMB
AQAECDAGAQH/AgEBMAOGCSqGSIb3DQEBBQUAA0EANTZmrAGGFBCpii/UReywyGCT
2bUb1Zs93XPz86bYrg4YMTFNiHVbeoMo2uOYAMpk3yuTZuaf3SgEEnz8wGZ8JA==
-----END CERTIFICATE-----

```

The following table describes the labels in this screen.

Table 69 My Certificate Details

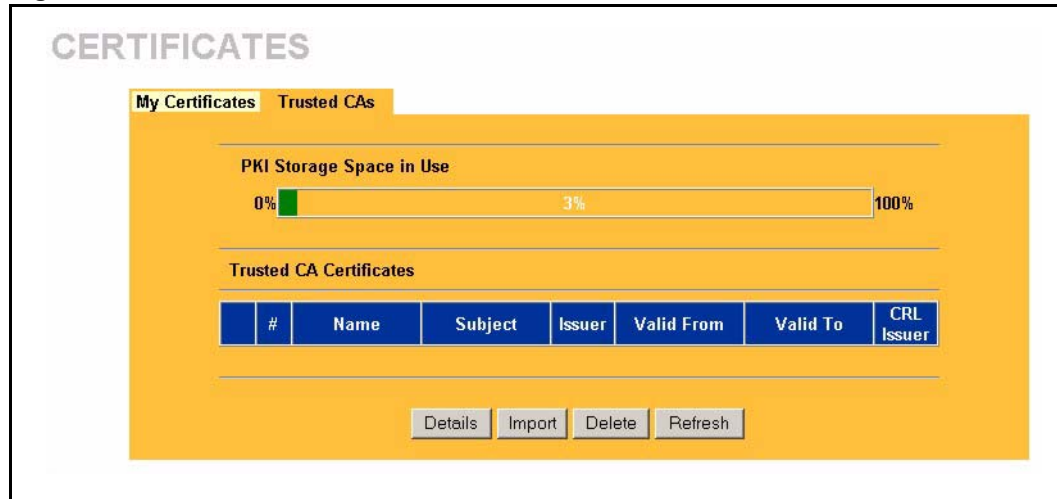
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyAIR use this certificate to sign the trusted remote host certificates that you import to the ZyAIR. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certificate Path	Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyAIR does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyAIR.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyAIR uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyAIR uses RSA encryption) and the length of the key set in bits (1024 bits for example).

Table 69 My Certificate Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export	<p>Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.</p> <p>Note: When you are saving your certificate, use "cer" or "cert" as the file name extension.</p>
Apply	Click Apply to save your changes back to the ZyAIR. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click Cancel to quit and return to the My Certificates screen.

17.9 Trusted CAs

Click **CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyAIR to accept as trusted. The ZyAIR accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. See the following figure.

Figure 95 Trusted CAs

The following table describes the labels in this screen.

Table 70 Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyAIR's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the Issues certificate revocation lists (CRL) check box in the certificate's details screen to have the ZyAIR check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Details	Click Details to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyAIR to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Table 70 Trusted CAs (continued)

LABEL	DESCRIPTION
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyAIR.
Delete	Click Delete to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click this button to display the current validity status of the certificates.

17.10 Importing a Trusted CA's Certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyAIR, see the following figure.



Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 96 Trusted CA Import

CERTIFICATES

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

The following table describes the labels in this screen.

Table 71 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the ZyAIR.
Cancel	Click Cancel to quit and return to the Trusted CAs screen.

17.11 Trusted CA Certificate Details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyAIR to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 97 Trusted CA Details

CERTIFICATES

Name

auto_generated_self_signed_cert

Property

☒ Default self-signed certificate which signs the imported remote host certificates.

Certificate Path

Searching...

Refresh

Certificate Information

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946684804
Subject	CN=ZyAIR G-2000PLUS Factory Default Certificate
Issuer	CN=ZyAIR G-2000PLUS Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=factory@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	ae:96:ec:3c:31:5f:47:6a:a8:cd:cd:8d:e8:89:9a:9c
SHA1 Fingerprint	29:c5:8f:be:64:2d:1d:1f:4f:f5:20:d7:51:ad:86:e6:77:85:63:cc

Certificate in PEM (Base-64) Encoded Format

```

MIIBqjCCAVSgAwIBAgIEOG1DhDANBgkqhkiG9w0BAQUFADA3MTUwMwYDVQQDEYxa
eUFUJUIBHLTIwMDEBQTFVTIEZyY3RvcnkgRGVmYXVsdCBDZXJ0aWZpY2F0ZTAeFw0w
MDAxMDEwMDAwMDEBaFw0ZMDAxMDEwMDAwMDEBaNDcxNTAaBgNVBAMTLFp5SQU1SIEct
MjAaMFBNVWVhZmFjdG9yeSBZW2h0dX01EN1cnRpZmljYXR1MFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAAKcg/9pDXyhyWIEpJ3PV/ONdIbClz67qDE2p30zNNuz5SkH2
qetvotua10+1lf6xWA57Yr5tWAGnV4EQoZsRuMCAwEAAANIMEYwDgYDVROPAQEA
BAQDAGkKHCAGA1UdeEQZMBEwFwZyY3Rvcn1AYXV0b35nZW4uY2VydDASBgNVHRMB
AQAECDAGAQH/AgEBMAOGCSqGSIb3DQEBBQUAAOEANTZmrAGGFBCp1i/URewyGCT
2hUb1Zs93XPz86bYrg4YMTFN1HvbeoMo2uYAMpk3yuT2uaf3SgEEnz8wGZ8JA==
-----END CERTIFICATE-----

```

Export

Apply

Cancel

The following table describes the labels in this screen.

Table 72 Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyAIR use this certificate to sign the trusted remote host certificates that you import to the ZyAIR. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certificate Path	Click the Refresh button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyAIR does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

Table 72 Trusted CA Details (continued)

LABEL	DESCRIPTION
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyAIR uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes back to the ZyAIR. You can only change the name and/or set whether or not you want the ZyAIR to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click Cancel to quit and return to the Trusted CAs screen.

CHAPTER 18

Log Screens

This chapter contains information about configuring general log settings and viewing the ZyAIR's logs. Refer to the appendix for example log message explanations.

18.1 Configuring View Log

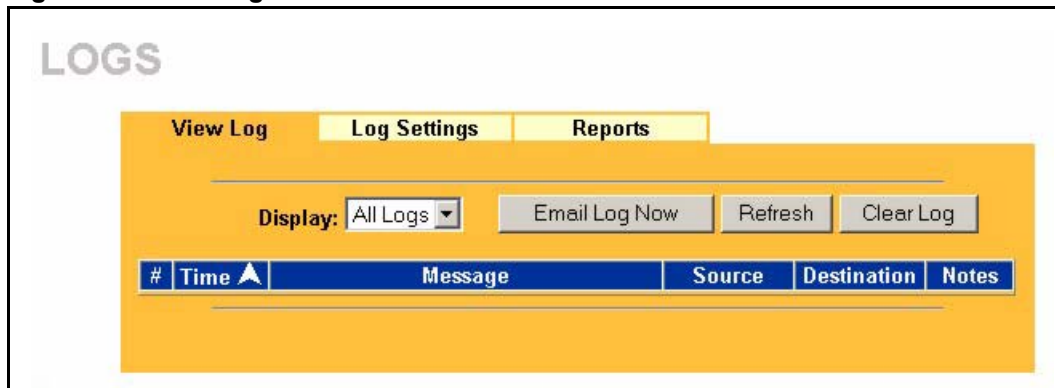
The web configurator allows you to look at all of the ZyAIR's logs in one location.

Click the **LOGS** links under **ADVANCED** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Figure 99](#)). Options include logs about system maintenance, system errors and access control.

You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

Figure 98 View Log



The following table describes the labels in this screen.

Table 73 View Log

LABEL	DESCRIPTION
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select All Logs . The number of categories shown in the drop down list box depends on the selection in the Log Settings page.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.

Table 73 View Log

LABEL	DESCRIPTION
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Settings page.
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to clear all the logs.

18.2 Configuring Log Settings

To change your ZyAIR's log settings, click the **LOGS** links under **ADVANCED** and then the **Log Settings** tab. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyAIR is to send the logs; the schedule for when the ZyAIR is to send the logs and which logs and/or immediate alerts the ZyAIR is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

Figure 99 Log Settings

Log Settings

View Log
Log Settings
Reports

Address Info:

Mail Server: (Outgoing SMTP Server NAME or IP Address)

Mail Subject:

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

Syslog Logging:

☐ Active

Syslog IP Address: (Server NAME or IP Address)

Log Facility:

Send Log:

Log Schedule:

Day for Sending Log:

Time for Sending Log: (hour) (minute)

☐ Clear log after sending mail

Log

☐ System Maintenance

☐ System Errors

☐ Access Control

☐ TCP Reset

☐ Packet Filter

☐ ICMP

☐ Remote Management

☐ CDR

☐ PPP

☐ UPnP

☐ Forward Web Sites

☐ Blocked Web Sites

☐ Blocked Java etc.

☐ Attacks

☐ PKI

☐ SSL/TLS

☐ 802.1x

☐ Wireless

☐ Internal RADIUS Server

Send immediate alert

☐ System Errors

☐ Access Control

☐ Blocked Web Sites

☐ Blocked Java etc.

☐ Attacks

☐ PKI

The following table describes the labels in this screen.

Table 74 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyAIR sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click Active to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If the Weekly or the Daily option is selected, specify a time of day when the E-mail should be sent. If the Weekly option is selected, then also specify which day of the week the E-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	This field is only available when you select Weekly in the Log Schedule field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select the categories of alerts for which you want the ZyAIR to immediately send e-mail alerts.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to reconfigure all the fields in this screen.

18.3 Configuring Reports

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. Use the **Reports** screen to have the ZyAIR record and display the following network usage details:

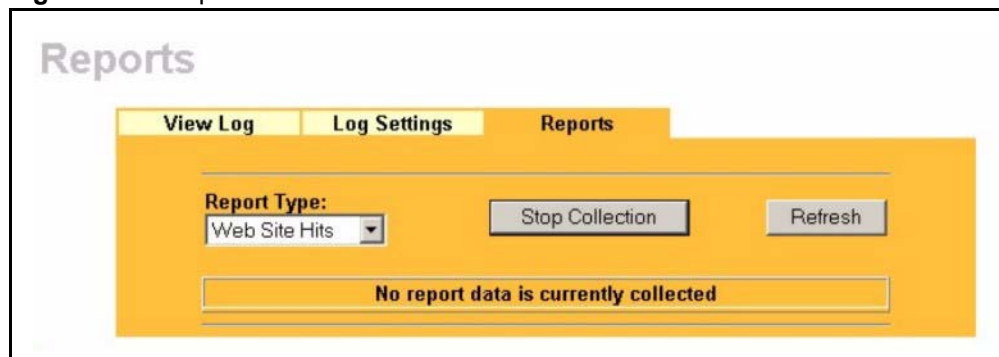
- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN IP addresses to and/or from which the most traffic has been sent



Note: The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

The ZyAIR records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the ZyAIR may count these as hits, thus the web hit count is not (yet) 100% accurate.

To change your ZyAIR's log reports, click **LOGS**, then the **Reports** tab. The screen appears as shown.

Figure 100 Reports

Note: Enabling the ZyAIR's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the labels in this screen.

Table 75 Reports

LABEL	DESCRIPTION
Report Type	Use the drop-down list box to select the type of reports to display. Web Site Hits displays the web sites that have been visited the most often from the LAN and how many times they have been visited. Protocol/Port displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. LAN IP Address displays the LAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Start Collection Stop Collection	The button text shows Start Collection when the ZyAIR is not recording report data and Stop Collection when the ZyAIR is recording report data. Click Start Collection to have the ZyAIR record report data. Click Stop Collection to halt the ZyAIR from recording more data.
Refresh	Click Refresh to update the report display. The report also refreshes automatically when you close and reopen the screen.
#	This field displays the index number of an individual web site.
Web Site	Web Site displays the web site address(es) that have been visited the most often from the LAN.
Hits	Hits displays the total number of visits to each web site.
Direction	This field displays Incoming to denote traffic that is coming in from the WAN to the LAN. This field displays Outgoing to denote traffic that is going out from the LAN to the WAN.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit.
IP Address	This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and/or from which the most traffic was sent listed first.



Note: All of the recorded reports data is erased when you turn off the ZyAIR.

CHAPTER 19

Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

19.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyAIR.

19.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can use to monitor your ZyAIR. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.

Figure 101 System Status

SYSTEM STATUS

Status | DHCP Table | Association List | F/W Upload | Configuration | Restart

System Name : G-2000PLUS

Model Name : ZyAIR G-2000PLUS
ZyNOS Firmware Version: V3.60(HU.0)b5 | 11/30/2004

WAN Port :

IP Address : 0.0.0.0 DHCP : Client
IP Subnet Mask : 0.0.0.0

LAN Port :

IP Address : 192.168.1.1 DHCP : Server
IP Subnet Mask : 255.255.255.0

Show Statistics

The following table describes the labels in this screen.

Table 76 System Status

LABEL	DESCRIPTION
System Name	This is the System Name you chose in the first Internet Access Wizard screen. It is for identification purposes
Model Name	The model name identifies your device type. The model name should also be on a sticker on your ZyAIR. If you are uploading firmware, be sure to upload firmware for this exact model name. This field is not available on all models.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - Client or None .
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - Server , Relay or None .
Show Statistics	Click Show Statistics to display the real-time system statistics. For more information see System Statistics on page 242.

19.2.1 System Statistics

Read-only information here includes port status, packet specific statistics and bridge link status. Also provided are "system up time" and "poll interval(s)". The **Poll Interval** field is configurable.

Figure 102 System Status: Show Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	822	875	0	0	0	0:04:29
WLAN	54M	60	0	0	0	0	0:04:30

System Up Time : 0:04:36

Poll Interval(s) : **sec**

The following table describes the labels in this screen.

Table 77 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the WAN, LAN or WLAN port.
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. This shows the transmission speed only for wireless port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is total amount of time the line has been up.
System Up Time	This is the total time the ZyAIR has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

19.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyAIR as a DHCP server or disable it. When configured as a server, the ZyAIR provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

Figure 103 Maintenance DHCP Table

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	tw11477-02	00:50:8d:48:59:1f	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 78 Maintenance DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the Host Name field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this check box to have the ZyAIR always assign this IP address to this MAC address (and host name).
Apply	Click Apply to have the MAC address and IP address also display in the LAN Static DHCP screen (where you can edit them).
Refresh	Click Refresh to renew the screen.

19.4 Association List

View the wireless stations that are currently associated to the ZyAIR in the **Association List** screen.

Click **MAINTENANCE** and then the **Association List** tab to display the screen as shown next.

Figure 104 Association List

WIRELESS											
Status	DHCP Table	Association List									
		<table border="1"> <thead> <tr> <th>#</th> <th>MAC Address</th> <th>Association Time</th> </tr> </thead> <tbody> <tr> <td>001</td> <td>00:a0:c5:b6:0b:b8</td> <td>00:00:55 2000/01/01</td> </tr> <tr> <td>002</td> <td>00:a0:c5:80:f5:fa</td> <td>00:08:06 2000/01/01</td> </tr> </tbody> </table>	#	MAC Address	Association Time	001	00:a0:c5:b6:0b:b8	00:00:55 2000/01/01	002	00:a0:c5:80:f5:fa	00:08:06 2000/01/01
#	MAC Address	Association Time									
001	00:a0:c5:b6:0b:b8	00:00:55 2000/01/01									
002	00:a0:c5:80:f5:fa	00:08:06 2000/01/01									
		Refresh									

The following table describes the labels in this screen.

Table 79 Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyAIR.
Refresh	Click Refresh to reload the screen.

19.5 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "zyair.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the *Firmware and Configuration File Maintenance* chapter for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** and then **F/W Upload**. Follow the instructions in this screen to upload firmware to your ZyAIR.

Figure 105 Firmware Upload

The following table describes the labels in this screen.

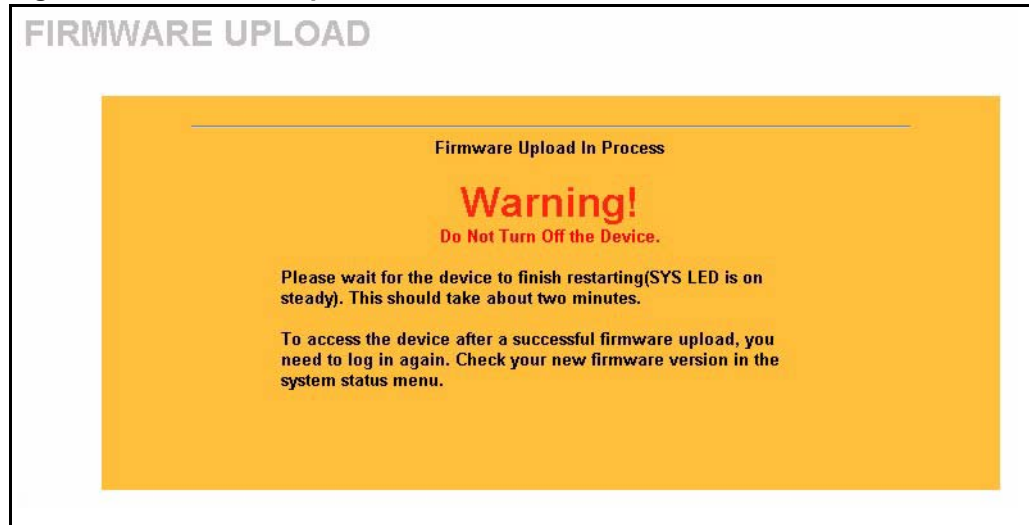
Table 80 Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

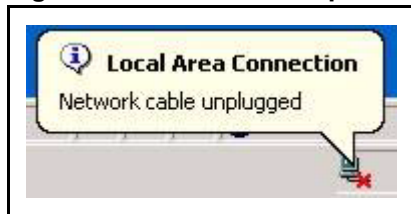


Note: Do not turn off the ZyAIR while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyAIR again.

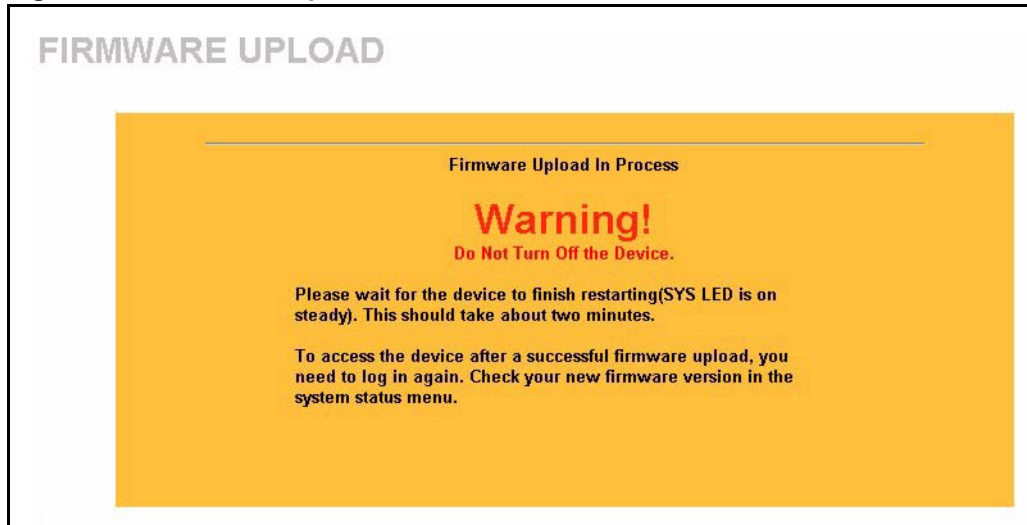
Figure 106 Firmware Upload In Process

The ZyAIR automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 107 Network Temporarily Disconnect

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 108 Firmware Upload Error

19.6 Configuration Screen

See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 109 Configuration

MAINTENANCE

Status DHCP Table Association List F/W Upload **Configuration** Restart

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Backup

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path: Browse...

Upload

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Reset

19.6.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyAIR's current configuration to a file on your computer. Once your ZyAIR is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyAIR's current configuration to your computer.

19.6.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyAIR.

Table 81 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.

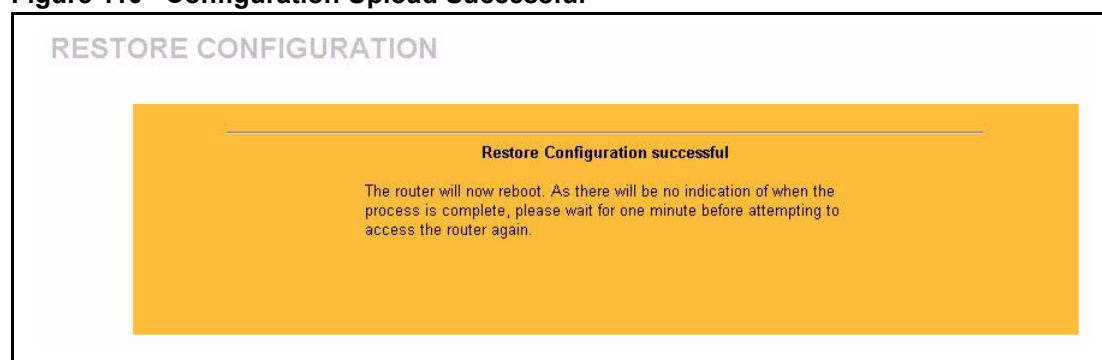
Table 81 Restore Configuration

LABEL	DESCRIPTION
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin the upload process.

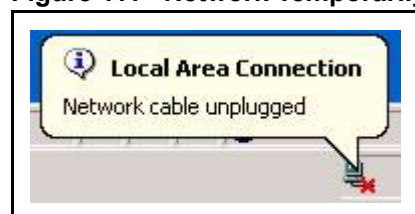


Note: Do not turn off the ZyAIR while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyAIR again.

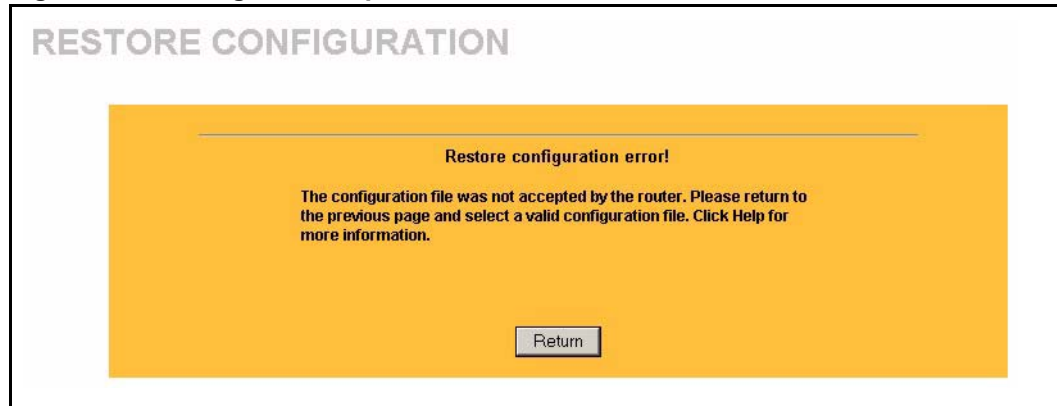
Figure 110 Configuration Upload Successful

The ZyAIR automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 111 Network Temporarily Disconnected

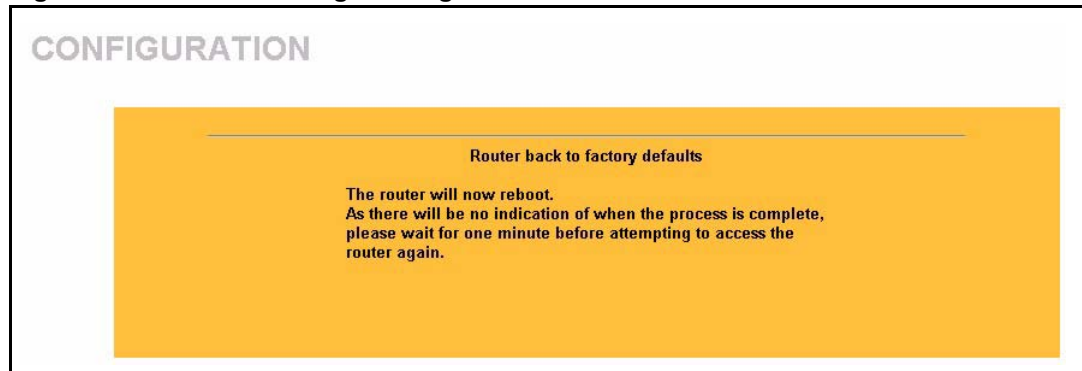
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyAIR IP address (192.168.1.1). See your *Quick Installation Guide* for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 112 Configuration Upload Error

19.6.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyAIR to its factory defaults as shown on the screen. The following warning screen will appear.

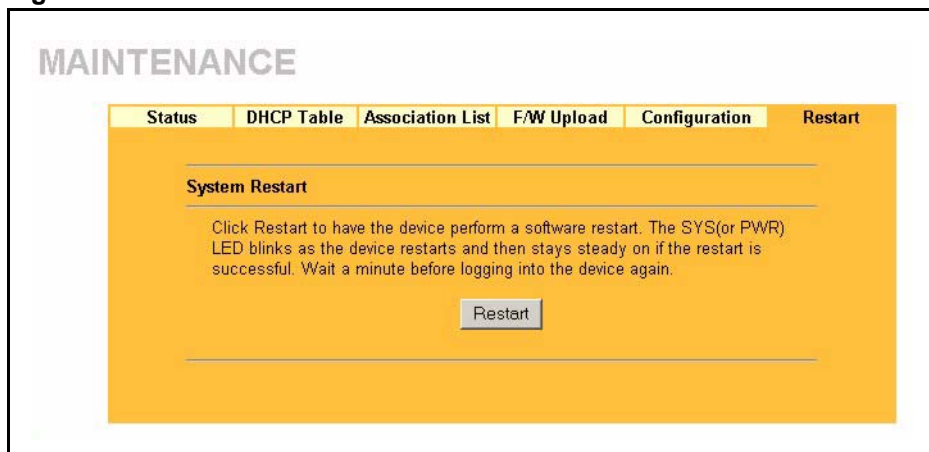
Figure 113 Reset Warning Message

You can also press the **RESET** button on the side panel to reset the factory defaults of your ZyAIR. Refer to the section on resetting the ZyAIR for more information on the **RESET** button.

19.7 Restart Screen

System restart allows you to reboot the ZyAIR without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the ZyAIR reboot. This does not affect the ZyAIR's configuration.

Figure 114 Restart Screen

CHAPTER 20

Introducing the SMT

This chapter explains how to access and navigate the System Management Terminal and gives an overview of its menus.

20.1 SMT Introduction

The ZyAIR's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus, how to navigate the SMT and how to configure SMT menus.

20.2 Connect to your ZyAIR Using Telnet

The following procedure details how to telnet into your ZyAIR.

- 1 In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.
- 2 For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "*" for each character you type.

Figure 115 Login Screen

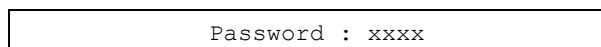


Figure 115 shows a screenshot of the login screen. It consists of a rectangular box with a thin black border. Inside the box, the text "Password : xxxx" is displayed in a monospaced font, where "xxxx" represents masked characters.

- 3 After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ZyAIR will automatically log you out. You will then have to telnet into the ZyAIR again. You can use the web configurator or the CI commands to change the inactivity time out period.

20.2.1 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "*" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your ZyAIR will automatically log you out.

Figure 116 Login Screen

Enter Password : ****

20.3 Changing the System Password

Change the ZyAIR default password by following the steps shown next.

- 1 From the main menu, enter 23 to display **Menu 23 – System Security**.
- 2 Enter 1 to display **Menu 23.1 – System Security – Change Password** as shown next.
- 3 Type your existing system password in the **Old Password** field, and press [ENTER].

Figure 117 Menu 23.1 System Security : Change Password

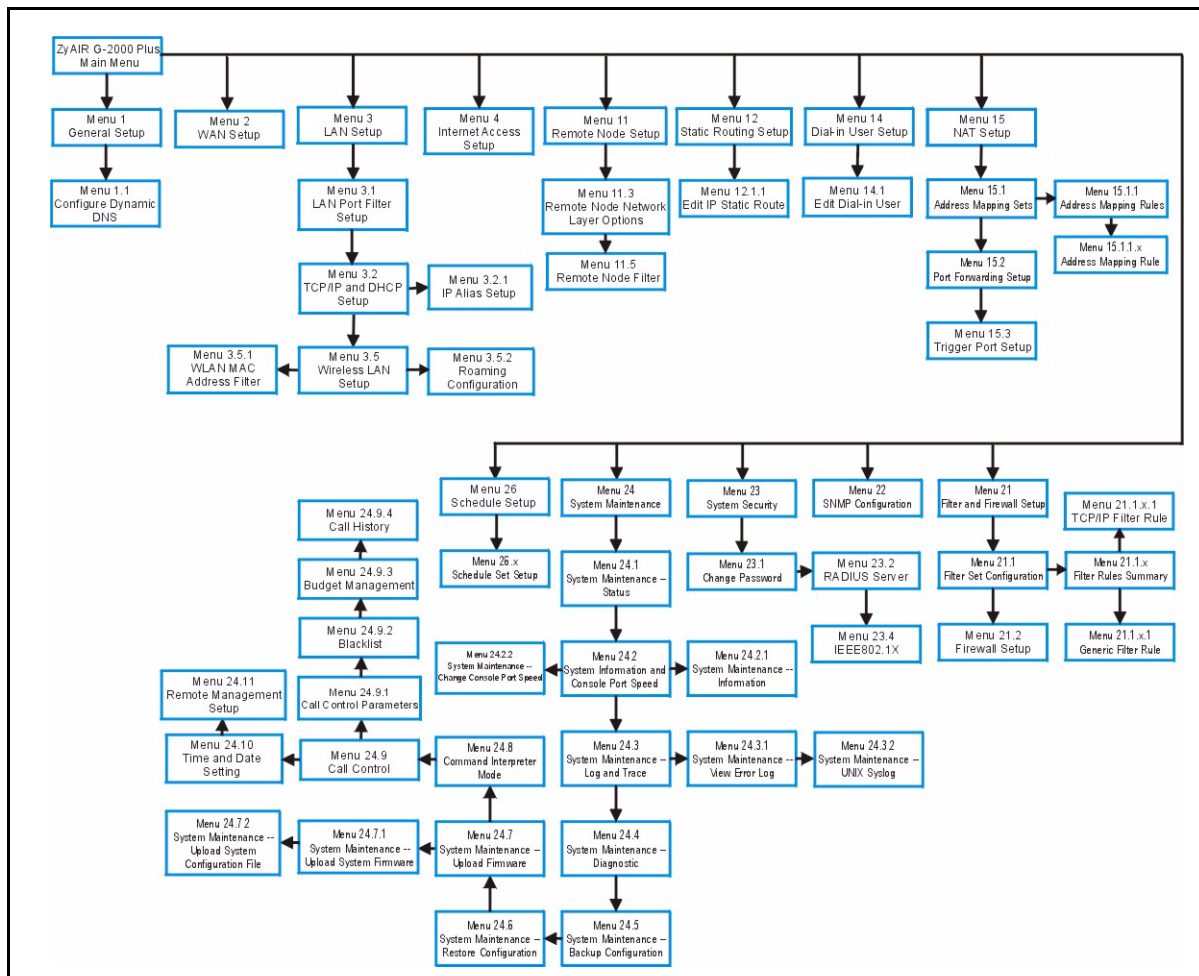
Menu 23.1 - System Security - Change Password Old Password= **** New Password= ? Retype to confirm= ? Enter here to CONFIRM or ESC to CANCEL:
--

- 4 Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
- 5 Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an asterisk “*” for each character you type.

20.4 ZyAIR SMT Menu Overview Example

The following figure gives you an example overview of the various SMT menu screens for your ZyAIR G-2000 Plus.

Figure 118 ZyAIR G-2000 Plus SMT Menu Overview Example

20.5 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyAIR.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 82 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.

Table 82 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move to a "hidden" menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of No . Press [SPACE BAR] once to change No to Yes , then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?> or ChangeMe	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with ChangeMe must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

Figure 119 ZyAIR G-2000 Plus SMT Main Menu

```

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

ZyAIR G-2000PLUS Main Menu

Getting Started
  1. General Setup
  2. WAN Setup
  3. LAN Setup
  4. Internet Access Setup

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  14. Dial-in User Setup
  15. NAT Setup

Advanced Management
  21. Filter and Firewall Setup
  22. SNMP Configuration
  23. System Security
  24. System Maintenance
  26. Schedule Setup

99. Exit

Enter Menu Selection Number:

```

20.5.1 System Management Terminal Interface Summary

Table 83 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Use this menu to set up static routes.
14	Dial-in User Setup	Use this menu to set up local user profiles on the ZyAIR.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

20.6 Changing the System Password

Change the ZyAIR default password by following the steps shown next.

- 1 Enter 23 in the main menu to display **Menu 23 - System Security** as shown next.

Figure 120 Menu 23: System Security

```
Menu 23 - System Security

1.  Change Password
2.  RADIUS Server
4.  IEEE802.1x
```

- 2 Enter 23.1 in the main menu to display **Menu 23.1 - System Security - Change Password**.

- 3 Type your existing system password in the **Old Password** field, for example “1234”, and press [ENTER]

Figure 121 Menu 23 System Password

```
Menu 23.1 - System Security - Change Password

Old Password= ?
New Password= ?
Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:
```

- 4 Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
- 5 Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].



Note: When you type in a password, the screen displays an “*” for each character typed

CHAPTER 21

General Setup

The chapter shows you the information on general setup.

21.1 General Setup

Menu 1 — General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the **ZyAIR System Name**.

In Windows 2000 click **Start, Settings, Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **ZyAIR System Name**.

In Windows XP, click **start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the **ZyAIR System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyAIR via DHCP.

21.1.1 Procedure To Configure Menu 1

Enter 1 in the Main Menu to open **Menu 1 – General Setup** as shown next.

Figure 122 Menu 1 General Setup

```

Menu 1 - General Setup

System Name= G-2000PLUS
Domain Name=

First System DNS Server= From ISP
IP Address= N/A
Second System DNS Server= From ISP
IP Address= N/A
Third System DNS Server= From ISP
IP Address= N/A
Edit Dynamic DNS= No

Press ENTER to Confirm or ESC to Cancel:

```

Fill in the required fields. Refer to the following table for more information about these fields.

Table 84 Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].
First System DNS Server Second System DNS Server Third System DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyAIR uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Press [SPACE BAR] and then [ENTER] to select an option. Select From ISP if your ISP dynamically assigns DNS server information (and the ZyAIR's WAN IP address). The IP Address field below displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the IP Address field. If you select User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you save your changes. If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you save your changes. Select None if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select Yes or No (default). Select Yes to configure Menu 1.1: Configure Dynamic DNS discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

21.1.2 Procedure to Configure Dynamic DNS



Note: If you have a private WAN IP address, then you cannot use Dynamic DNS

To configure Dynamic DNS, go to **Menu 1 — General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** as shown next.

Figure 123 Menu 1.1 Configure Dynamic DNS

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= No
DDNS Type= DynamicDNS
Host Name 1=
Host Name 2=
Host Name 3=
Username=
Password= *****
Enable Wildcard Option= No
Enable Off Line Option= N/A
IP Address Update Policy:
    DDNS Server Auto Detect IP Address= No
    Use Specified IP Address= No
    Use IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 85 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select Yes and then press [ENTER] to make dynamic DNS active.
DDNS Type	Press [SPACE BAR] and then [ENTER] to select DynamicDNS if you have a dynamic IP address(es). Select StaticDNS if you have a static IP address(s). Select CustomDNS to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.
Host 1- 3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.
User	Enter your user name.
Password	Enter the password assigned to you.

Table 85 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
Enable Wildcards	Your ZyAIR supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select Yes or No . This field is N/A when you choose DDNS client as your service provider.
Offline	This field is only available when CustomDNS is selected in the DDNS Type field. Press [SPACE BAR] and then [ENTER] to select Yes . When Yes is selected, http://www.dyndns.org/ traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).
Edit Update IP Address: You can select Yes in either the Use Server Detected IP field (recommended) or the User Specified IP Addr field, but not both. With the Use Server Detected IP and User Specified IP Addr fields both set to No , the DDNS server automatically updates the IP address of the host name(s) with the ZyAIR's WAN IP address. DDNS does not work with a private IP address. When both fields are set to No , the ZyAIR must have a public WAN IP address in order for DDNS to work.	
Use Server Detected IP	Press [SPACE BAR] to select Yes and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the ZyAIR uses or is behind. You can set this field to Yes whether the IP address is public or private, static or dynamic.
User Specified IP Address	Press [SPACE BAR] to select Yes and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select Yes if the ZyAIR uses or is behind a static public IP address.
IP Address	Enter the static public IP address if you select Yes in the User Specified IP Addr field.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	



Note: The IP address updates when you reconfigure menu 1 or perform DHCP client renewal

CHAPTER 22

Menu 2 WAN Setup

This chapter describes how to configure the WAN using menu 2.

22.1 Introduction to WAN

This chapter explains how to configure settings for your WAN port.

22.2 WAN Setup

From the main menu, enter 2 to open menu 2.

Figure 124 Menu 2 WAN Setup

Menu 2 - WAN Setup
MAC Address:
Assigned By= Factory default
IP Address= N/A

The following table describes the fields in this menu.

Table 86 Menu 2 WAN Setup

FIELD	DESCRIPTION
MAC Address	
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose Factory Default to select the factory assigned default MAC Address. Choose IP address attached on LAN to use the MAC Address of that computer whose IP you give in the following field.
IP Address	This field is applicable only if you choose the IP address attached on LAN method in the Assigned By field. Enter the IP address of the computer on the LAN whose MAC you are cloning.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 23

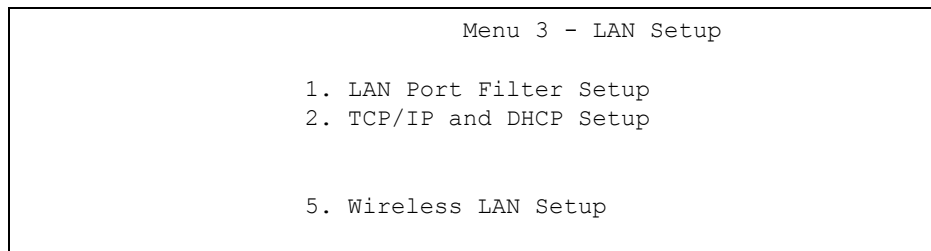
LAN Setup

This chapter shows you how to configure wired Local Area Network (LAN) settings on your ZyAIR..

23.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 – LAN Setup**. From the main menu, enter 3 to display menu 3.

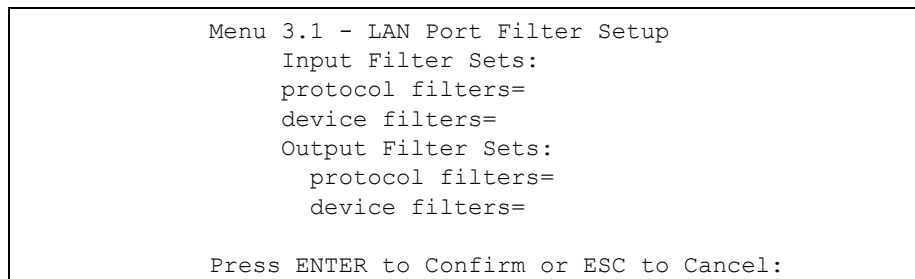
Figure 125 Menu 3 LAN Setup



23.1.1 General Ethernet Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches

Figure 126 Menu 3.1 LAN Port Filter Setup.



If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

23.2 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to the *Internet Access Application* chapter.
- For bridging Ethernet setup refer to the *Bridging Setup* chapter.

23.3 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your ZyAIR for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 — LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next:

Figure 127 Menu 3.2 TCP/IP Setup

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= Server                      TCP/IP Setup:
Client IP Pool:
    Starting Address= 192.168.1.33  IP Address= 192.168.1.1
    Size of Client IP Pool= 32      IP Subnet Mask= 255.255.255.0
First DNS Server= From ISP          RIP Direction= Both
    IP Address= N/A                 Version= RIP-1
Second DNS Server= From ISP          Multicast= None
    IP Address= N/A                 Edit IP Alias= No
Third DNS Server= From ISP
    IP Address= N/A
DHCP Server Address= N/A

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

Follow the instructions in the next table on how to configure the DHCP fields.

Table 87 DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
DHCP	This field enables/disables the DHCP server. If set to Server , your ZyAIR will act as a DHCP server. If set to None , the DHCP server will be disabled. If set to Relay the ZyAIR acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to Server , the following items need to be set:
Client IP Pools	
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.

Table 87 DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.
First DNS Server Second DNS Server Third DNS Server	<p>The ZyAIR passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients.</p> <p>Select From ISP if your ISP dynamically assigns DNS server information (and the ZyAIR's WAN IP address). The IP Address field below displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the IP Address field below. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you save your changes. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you save your changes.</p> <p>Select DNS Relay to have the ZyAIR act as a DNS proxy. The ZyAIR's LAN IP address displays in the IP Address field below (read-only). The ZyAIR tells the DHCP clients on the LAN that the ZyAIR itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyAIR, the ZyAIR forwards the query to the ZyAIR's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you save your changes.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p>
DHCP Server Address	If Relay is selected in the DHCP field above, then type the IP address of the actual, remote DHCP server here.

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

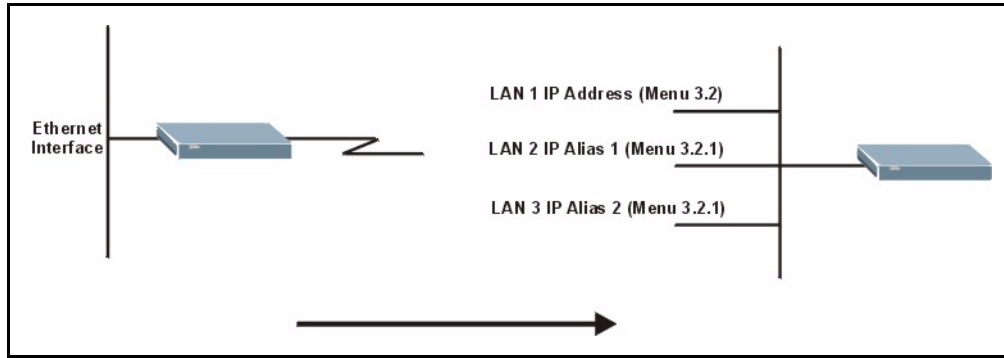
Table 88 Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION
TCP/IP Setup:	
IP Address	Enter the IP address of your ZyAIR in dotted decimal notation
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: Both , In Only , Out Only or None .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: RIP-1 , RIP-2B or RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyAIR supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select None (default) to disable it.
Edit IP Alias	The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network. Press [SPACE BAR] to select Yes and then press [ENTER] to display menu 3.2.1
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	

23.3.1 IP Alias Setup

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network.

Figure 128 Physical Network & Partitioned Logical Networks



You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

Figure 129 Menu 3.2.1: IP Alias Setup

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A
IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

```

Use the instructions in the following table to configure IP alias parameters.

Table 89 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose Yes to configure the LAN network for the ZyAIR.
IP Address	Enter the IP address of your ZyAIR in dotted decimal notation.
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are Both , In Only , Out Only or None .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are RIP-1 , RIP-2B or RIP-2M .
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyAIR.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyAIR.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	

23.4 Wireless LAN Setup

Use menu 3.5 to set up your ZyAIR as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

Figure 130 Menu 3.5 Wireless LAN Setup

```

Menu 3.5 - Wireless LAN Setup

Enable Wireless LAN= Yes
ESSID= Wireless
Hide ESSID= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= 128-bit WEP
    Default Key= 1
    Key1= *****
    Key2= *****
    Key3= *****
    Key4= *****
    Authen. Method= Auto
Edit MAC Address Filter= No
Edit Roaming Configuration= No
Breathing LED= Yes
Preamble= Long
802.11 Mode= Mixed

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

The following table describes the fields in this menu.

Table 90 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.
Hide ESSID	Press [SPACE BAR] and select Yes to hide the ESSID in the outgoing data frame so an intruder cannot obtain the ESSID through passive scanning.
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.
Fragment Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
WEP Encryption	Select Disable to allow wireless stations to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyAIR and the wireless stations to communicate.

Table 90 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose 64-bit WEP in the WEP Encryption field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP in the WEP Encryption field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>Note: Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key</p>
Authen. Method	<p>Press [SPACE BAR] to select Auto, Open System Only or Shared Key Only and press [ENTER].</p> <p>This field is N/A if WEP is not activated.</p> <p>If WEP encryption is activated, the default setting is Auto.</p>
Edit MAC Address Filter	See the following section for details on this field.ZyAIR
Edit Roaming Configuration	<p>Press [SPACE BAR] to select Yes to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet.</p> <p>Note: All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming.</p>
Breathing LED	<p>Select Yes to enable the Breathing LED, also known as the ZyAIR LED.</p> <p>The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.</p>
Preamble	<p>Press [SPACE BAR] to select a preamble type. Choices are Long, Short and Dynamic. The default setting is Long.</p> <p>See the section on preamble for more information.</p>
802.11 Mode	<p>Press [SPACE BAR] to select B Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR.</p> <p>Select G Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR.</p> <p>Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

23.4.1 Configuring MAC Address Filter

Your ZyAIR checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyAIR.

- 1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 131 Menu 3.5 Wireless LAN Setup

Menu 3.5 - Wireless LAN Setup	
Enable Wireless LAN= Yes	
ESSID= Wireless	
Hide ESSID= No	Edit MAC Address Filter= Yes
Channel ID= CH06 2437MHz	Edit Roaming Configuration= No
RTS Threshold= 2432	Breathing LED= Yes
Frag. Threshold= 2432	Preamble= Long
WEP Encryption= 128-bit WEP	802.11 Mode= Mixed
Default Key= 1	
Key1= *****	
Key2= *****	
Key3= *****	
Key4= *****	
Authen. Method= Shared Key Only	

3 In the **Edit MAC Address Filtering** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 – WLAN MAC Address Filter** displays as shown next.

Figure 132 Menu 3.5.1 WLAN MAC Address Filter

Menu 3.5.1 - WLAN MAC Address Filter					
Active= No					
Filter Action= Allowed Association					

1=	00:00:00:00:00:00	13=	00:00:00:00:00:00	25=	00:00:00:00:00:00
2=	00:00:00:00:00:00	14=	00:00:00:00:00:00	26=	00:00:00:00:00:00
3=	00:00:00:00:00:00	15=	00:00:00:00:00:00	27=	00:00:00:00:00:00
4=	00:00:00:00:00:00	16=	00:00:00:00:00:00	28=	00:00:00:00:00:00
5=	00:00:00:00:00:00	17=	00:00:00:00:00:00	29=	00:00:00:00:00:00
6=	00:00:00:00:00:00	18=	00:00:00:00:00:00	30=	00:00:00:00:00:00
7=	00:00:00:00:00:00	19=	00:00:00:00:00:00	31=	00:00:00:00:00:00
8=	00:00:00:00:00:00	20=	00:00:00:00:00:00	32=	00:00:00:00:00:00
9=	00:00:00:00:00:00	21=	00:00:00:00:00:00		
10=	00:00:00:00:00:00	22=	00:00:00:00:00:00		
11=	00:00:00:00:00:00	23=	00:00:00:00:00:00		
12=	00:00:00:00:00:00	24=	00:00:00:00:00:00		

Enter here to CONFIRM or ESC to CANCEL:					
Press Space Bar to Toggle.					

The following table describes the fields in this menu.

Table 91 Menu 3.5.1 WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select Yes and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the ZyAIR, press [SPACE BAR] to select Deny Association and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, Allowed Association , permits association with the ZyAIR. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
1..32	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyAIR in these address fields.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 24

Internet Access

This chapter shows you how to configure your ZyAIR for Internet access .

24.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your ZyAIR to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

24.2 Ethernet Encapsulation

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**.

If you choose **Ethernet** in menu 4 you will see the next menu.

Figure 133 Menu 4 Internet Access Setup

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

Table 92 Internet Access Setup (Ethernet

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose Ethernet . The encapsulation method influences your choices for the IP Address field.
Service Type	Press [SPACE BAR] and then [ENTER] to select Standard , RR-Toshiba (RoadRunner Toshiba authentication method), RR-Manager (RoadRunner Manager authentication method), RR-Telstra or Telia Login . Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose Standard .
Note: DSL users must choose the Standard option only. The My Login , My Password and Login Server fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Type your password again for confirmation.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The ZyAIR will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
Relogin Every (min)	This field is available when you select Telia Login in the Service Type field. The Telia server logs the ZyAIR out if the ZyAIR does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyAIR to wait between logins.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select Dynamic , otherwise select Static and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).

Table 92 Internet Access Setup (Ethernet (continued))

FIELD	DESCRIPTION
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose None to disable NAT.</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p> <p>Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many- One-to-One and Server. When you select Full Feature you must configure at least one address mapping set!</p> <p>Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

24.3 Configuring the PPTP Client



Note: The ZyAIR supports only one PPTP server connection at any given time

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

Figure 134 Internet Access Setup (PPTP)

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPTP
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 93 New Fields in Menu 4 (PPTP) Screen

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose PPTP . The encapsulation method influences your choices for the IP Address field.
Idle Timeout	This value specifies the time, in seconds, that elapses before the ZyAIR automatically disconnects from the PPTP server.

24.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the appendix.

Figure 135 Internet Access Setup (PPPoE)

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPPoE
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

Table 94 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose PPPoE . The encapsulation method influences your choices in the IP Address field.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyAIR automatically disconnects from the PPPoE server.

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

24.5 Basic Setup Complete

Well done! You have successfully connected, installed and set up your ZyAIR to operate on your network as well as access the Internet.



Note: When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the ZyAIR embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

CHAPTER 25

Remote Node Configuration

This chapter covers remote node configuration.

25.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options**, **Menu 11.5 - Remote Node Filter**.

25.2 Remote Node Profile Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Profile** (shown below).

The following explains how to configure the remote node profile menu.

25.2.1 Ethernet Encapsulation

There are two variations of menu 11 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

Figure 136 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe      Route= IP
Active= Yes                  ISP= No
                             Apply Alias= None
Encapsulation= Ethernet      Edit IP= No
Service Type= Standard       Session Options:
Service Name= N/A           Edit Filter Sets= No
Outgoing:
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Server= N/A
  Relogin Every (min)= N/A

Press ENTER to Confirm or ESC to Cancel:
Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

Table 95 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select Yes (activate remote node) or No (deactivate remote node).
Encapsulation	Ethernet is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to PPPoE or PPTP encapsulation.
Service Type	Press [SPACE BAR] and then [ENTER] to select from Standard , RR-Toshiba (RoadRunner Toshiba authentication method), RR-Manager (RoadRunner Manager authentication method), RR-Telstra or Telia Login . Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose Standard .
Outgoing	
My Login	This field is applicable for PPPoE encapsulation only. Enter the login name assigned by your ISP when the ZyAIR calls this remote node. Some ISPs append this field to the Service Name field above (e.g., jim@poellc) to access the PPPoE server.
My Password	Enter the password assigned by your ISP when the ZyAIR calls this remote node. Valid for PPPoE encapsulation only.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Server	This field is valid only when RoadRunner is selected in the Service Type field. The ZyAIR will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.
Relogin Every (min)	This field is available when you select Telia Login in the Service Type field. The Telia server logs the ZyAIR out if the ZyAIR does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyAIR to wait between logins.

Table 95 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
Route	This field refers to the protocol that will be routed by your ZyAIR – IP is the only option for the ZyAIR.
ISP	Use [SPACE BAR] to select Yes to use your ISP.
Apply Alias	The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network. Press [SPACE BAR] to select IP Alias 1 or 2 and then press [ENTER].
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select Yes and press [ENTER] to go to Menu 11.3 - Remote Node Network Layer Options .
Session Options	
Edit Filter Sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select Yes and press [ENTER] to open menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

25.2.2 PPPoE Encapsulation

The ZyAIR supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the ZyAIR with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE**, then you will see the next screen. Please see the appendix for more information on PPPoE.

Figure 137 Menu 11.1 Remote Node Profile for PPPoE Encapsulation

```
Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe          Route= IP
Active= Yes                      ISP= No
                                 Apply Alias= None
Encapsulation= PPPoE             Edit IP= No
Service Type= Standard           Telco Option:
Service Name=                    Allocated Budget(min)= 0
Outgoing:                        Period(hr)= 0
  My Login=                      Schedules=
  My Password= *****          Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

                                 Session Options:
                                 Edit Filter Sets= No
                                 Idle Timeout(sec)= 100

                                 Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

25.2.2.1 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

25.2.2.2 Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyAIR does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyAIR will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in [see Table 95](#).

Table 96 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION
Service Name	If you are using PPPoE encapsulation, then type the name of your PPPoE service here. Only valid with PPPoE encapsulation.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: <ul style="list-style-type: none"> • CHAP/PAP - Your ZyAIR will accept either CHAP or PAP when requested by this remote node. • CHAP- accept CHAP only. • PAP- accept PAP only.
Telco Option	
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the Allocated Budget is (10 minutes) and the Period(hr) is 1 (hour).
Schedules	You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup</i> chapter.
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.
Session Options	
Idle Timeout	Type the length of idle time (when there is no traffic from the ZyAIR to the remote node) in seconds that can elapse before the ZyAIR automatically disconnects the PPPoE connection. This option only applies when the ZyAIR initiates the call.

25.2.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the appendix for information on PPTP.

Figure 138 Menu 11.1 Remote Node Profile for PPTP Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe          Route= IP
Active= Yes                      ISP= No
                                 Apply Alias= None
Encapsulation= PPTP              Edit IP= No
Service Type= Standard           Telco Option:
Service Name= N/A                Allocated Budget(min)= 0
Outgoing:                        Period(hr)= 0
    My Login=                     Schedules=
    My Password= *****         Nailed-Up Connection= No
    Retype to Confirm= *****
    Authen= CHAP/PAP
PPTP My IP: Static               Session Options:
    My IP Addr=                   Edit Filter Sets= No
    My IP Mask=                   Idle Timeout(sec)= 100
    Server IP Addr=
    Connection ID/Name=

                                Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

The next table shows how to configure fields in menu 11.1 not previously discussed.

Table 97 Menu 11.1 Remote Node Profile for PPTP Encapsulation

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then [ENTER] to select PPTP . You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.
My IP Addr	Enter the IP address of the WAN Ethernet port.
My IP Mask	Enter the subnet mask of the WAN Ethernet port.
Server IP Addr	Enter the IP address of the ANT modem.
Connection ID/ Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format. This field is optional and depends on the requirements of your DSL modem.

25.3 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

Figure 139 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation

Menu 11.3 - Remote Node Network Layer Options	
IP Address Assignment=	Dynamic
Rem IP Addr=	N/A
Rem Subnet Mask=	N/A
My WAN Addr=	N/A
Network Address Translation=	SUA Only
Metric=	1
Private=	No
RIP Direction=	None
Version=	N/A
Multicast=	None

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

Table 98 Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select Dynamic ; otherwise select Static and enter the IP address & subnet mask in the following fields.
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.
Gateway IP Addr	This field is applicable to Ethernet encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.
My WAN Addr	This field is applicable to PPPoE and PPTP encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyAIR. Note that this is the address assigned to your local ZyAIR, not the remote router.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose None to disable NAT. Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server . Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One , Many-to-One (SUA/PAT), Many-to-Many Overload , Many- One-to-One and Server . When you select Full Feature you must configure at least one address mapping set! See the <i>NAT chapter</i> for a full discussion on this feature.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyAIR's routes (see the <i>Metric</i> section in the <i>WAN and Dial Backup Setup</i> chapter) The smaller the number, the higher priority the route has.

Table 98 Remote Node Network Layer Options

FIELD	DESCRIPTION
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from Both/ None/ In Only/Out Only . See the <i>LAN Setup</i> chapter for more information on RIP. The default for RIP on the WAN side is None . It is recommended that you do not change this setting.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from RIP-1/RIP-2B/ RIP-2M or None .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The ZyAIR supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press [SPACE BAR] to enable IP Multicasting or select None to disable it. See the <i>LAN Setup</i> chapter for more information on this feature.
Once you have completed filling in Menu 11.3 Remote Node Network Layer Options , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.	

25.4 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyAIR to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to the Filters chapter. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 140 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
protocol filters=
device filters=
Output Filter Sets:
protocol filters=
device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 141 Menu 11.5: Remote Node Filter (PPPoE and PPTP Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
protocol filters=
device filters=
Output Filter Sets:
protocol filters=
device filters=
Call Filter Sets:
protocol filters=
device filters=

Enter here to CONFIRM or ESC to CANCEL:
```


CHAPTER 26

Static Route Setup

This chapter shows how to setup IP static routes.

26.1 IP Static Route Setup

To configure an IP static route, use **Menu 12 – Static Routing Setup** (shown next).

Figure 142 Menu 12 IP Static Route Setup

Menu 12 - IP Static Route Setup

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

Enter selection number:

Now, type the route number of a static route you want to configure.

Figure 143 Menu12.1 Edit IP Static Route

```

Menu 12.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields for **Menu 12.1 – Edit IP Static Route Setup**.

Table 99 Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on <i>IP Subnet Mask</i> in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and is not included in RIP broadcasts. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 27

Dial-in User Setup

This chapter shows you how to create user accounts on the ZyAIR.

27.1 Dial-in User Setup

By storing user profiles locally, your ZyAIR is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your ZyAIR.

From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

Figure 144 Menu 14- Dial-in User Setup

Menu 14 - Dial-in User Setup			
1. aj tetryeg	9. _____	17. _____	25. _____
2. yeti 345	10. _____	18. _____	26. _____
3. 12345678901234+	11. _____	19. _____	27. _____
4. _____	12. _____	20. _____	28. _____
5. _____	13. _____	21. _____	29. _____
6. _____	14. _____	22. _____	30. _____
7. _____	15. _____	23. _____	31. _____
8. _____	16. _____	24. _____	32. _____
Enter Menu Selection Number:			

Type a number and press [ENTER] to edit the user profile.

Figure 145 Menu 14.1- Edit Dial-in User

```
Menu 14.1 - Edit Dial-in User

User Name= tester one
Active= Yes
Password= *****

Leave name field blank to delete profile
```

The following table describes the fields in this screen.

Table 100 Menu 14.1- Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select Yes and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 28

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyAIR.

28.1 Using NAT



Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyAIR

28.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See *section Address Mapping Sets* for a detailed description of the NAT set for SUA. The ZyAIR also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.



Note: Choose SUA Only if you have just one public WAN IP address for your ZyAIR.



Note: Choose Full Feature if you have multiple public WAN IP addresses for your ZyAIR.

28.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

Figure 146 Menu 4 Applying NAT for Internet Access

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= Full Feature

Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

- 1** Enter 11 from the main menu.
- 2** When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.
- 3** Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

Figure 147 Menu 11.3 Applying NAT to the Remote Node

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= None
    Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

```

The following table describes the options for Network Address Translation.

Table 101 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION
NAT	Press [SPACE BAR] and then [ENTER] to select Full Feature if you have multiple public WAN IP addresses for your ZyAIR. The SMT uses the address mapping set that you configure and enter in the Address Mapping Set field (menu 15.1 - see section).
	Select None to disable NAT.
	When you select SUA Only , the SMT uses Address Mapping Set 255 (menu 15.1 - see section). Choose SUA Only if you have just one public WAN IP address for your ZyAIR.

28.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 148 Menu 15 NAT Setup

```
Menu 15 - NAT Setup

1. Address Mapping Sets
2. Port Forwarding Setup
3. Trigger Port Setup

Enter Menu Selection Number:
```

28.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

Figure 149 Menu 15.1 Address Mapping Sets

```
Menu 15.1 - Address Mapping Sets

1. NAT_SET
255. SUA (read only)

Enter Menu Selection Number:
```

Enter 255 to display the next screen, [see the SUA \(Single User Account\) Versus NAT section](#). The fields in this menu cannot be changed.

Figure 150 Menu 15.1.255 SUA Address Mapping Rules

```

Menu 15.1.255 - Address Mapping Rules
Set Name= SUA
Idx  Local Start IP Local End IP      Global Start IP Global End IP   Type
---  -
1.   0.0.0.0        255.255.255.255  0.0.0.0         0.0.0.0         M-1
2.                                     0.0.0.0         Server
3.
4.
5.
6.
7.
8.
9.
10.

Press ENTER to Confirm or ESC to Cancel:

```

The following table explains the fields in this menu.

Table 102 SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	Local Start IP is the starting local IP address (ILA).
Local End IP	Local End IP is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP .
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types. Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	



Note: Menu 15.1.255 is read-only.

28.3.1.1 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

Figure 151 Menu 15.1.1 First Set

```

Menu 15.1.1 - Address Mapping Rules
Set Name= NAT_SET
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=
Press ENTER to Confirm or ESC to Cancel:

```



Note: If the Set Name field is left blank, the entire set will be deleted.



Note: The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here

28.3.1.2 Ordering Your Rules

Ordering your rules is important because the ZyAIR applies the rules in the order that you specify. When a rule matches the current packet, the ZyAIR takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 103 Menu 15.1.1 First Set

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is Edit . Edit means you want to edit a selected rule (see following field). Insert Before means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. Delete means to delete the selected rule and then all the rules after the selected one will be advanced one rule. None disables the Select Rule item.
Select Rule	When you choose Edit , Insert Before or Delete in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.



Note: You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.



Note: An End IP address must be numerically greater than its corresponding IP Start address

Figure 152 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 0.0.0.0
  End  = N/A

Global IP:
  Start= 0.0.0.0
  End  = N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table explains the fields in this menu.

Table 104 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. Server allows you to specify multiple servers of different types behind NAT to this computer. See <i>section</i> for an example.
Local IP	Only local IP fields are N/A for server; Global IP fields MUST be set for Server .
Start	This is the starting local IP address (ILA).
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is N/A for One-to-One and Server types.
Global IP	
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global IP Start . Note that Global IP Start can be set to 0.0.0.0 only if the types are Many-to-One or Server .

Table 104 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
End	This is the ending inside global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server types .
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

28.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

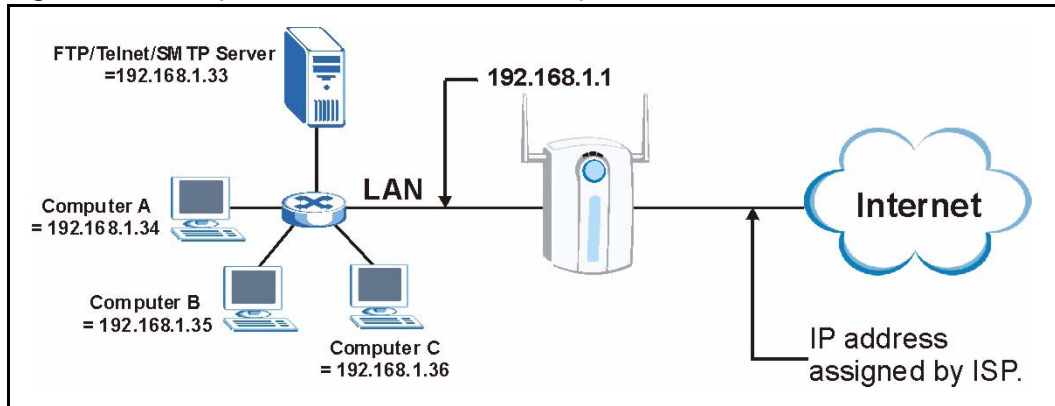
- 1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
- 2 Enter 2 to display **Menu 15.2 - NAT Server Setup** as shown next.

Figure 153 Menu 15.2.1 NAT Server Setup

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	21	25	192.168.1.33
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0
Press ENTER to Confirm or ESC to Cancel:			

- 3 Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.
- 4 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- 5 Press [ENTER] at the "Press ENTER to confirm ..." prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

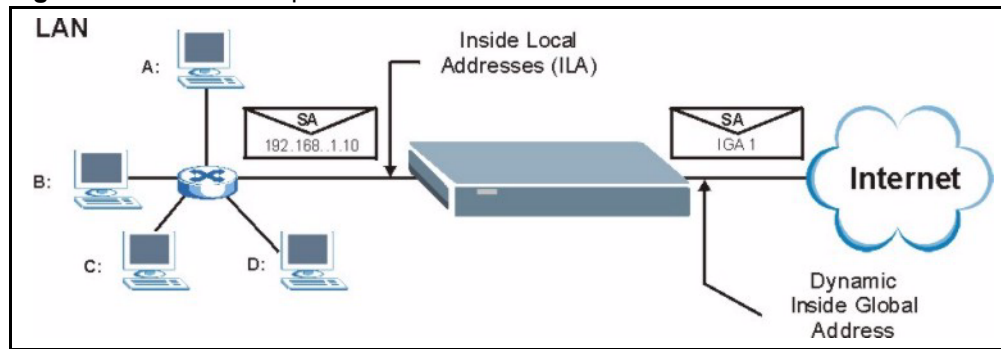
Figure 154 Multiple Servers Behind NAT Example

28.5 General NAT Examples

The following are some examples of NAT configuration.

28.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where the ILAs (Inside Local Addresses) of computers A through D map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 155 NAT Example 1**Figure 156** Menu 4 Internet Access & NAT Example

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
Press ENTER to Confirm or ESC to Cancel:

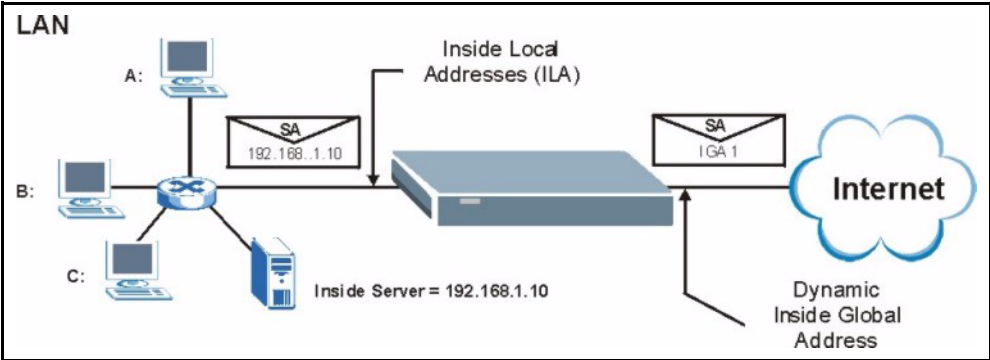
```

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section General NAT Examples*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

28.5.2 Example 2: Internet Access with an Inside Server

The dynamic Inside Global Address is assigned by the ISP.

Figure 157 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

Figure 158 Menu 15.2.1 Specifying an Inside Server

Menu 15.2.1 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	192.168.1.10
2.	0	0	0.0.0.0
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

28.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

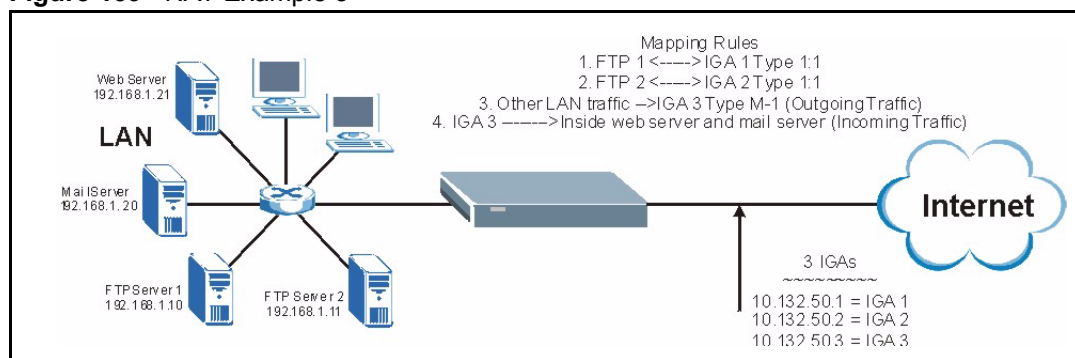
In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

- 1 Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- 2 Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- 3 Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

- 4 You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

Figure 159 NAT Example 3



- 1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) [see Figure 139](#).
- 2 Then enter 15 from the main menu.
- 3 Enter 1 to configure the Address Mapping Sets.
- 4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- 5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA) [see Figure 161](#).
- 6 Repeat the previous step for rules 2 to 4 as outlined above.
- 7 When finished, menu 15.1.1.1 should look like as shown in *Example 3: Final Menu 15.1.1*.

Figure 160 NAT Example 3: Menu 11.3

```
Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= 1
Private= N/A
RIP Direction= None
    Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

The following figures show how to configure the first rule.

Figure 161 Example 3: Menu 15.1.1.1

```

Menu 15.1.1.1 Address Mapping Rule
Type= One-to-One
Local IP:
  Start= 192.168.1.10
  End  = N/A
Global IP:
  Start= 10.132.50.1
  End  = N/A
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

Figure 162 Example 3: Final Menu 15.1.1

```

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   192.168.1.10    10.132.50.1    1-1
2.   192.168.1.11    10.132.50.2    1-1
3.   0.0.0.0         255.255.255.255 10.132.50.3     M-1
4.                                     10.132.50.3     Server
5.
6.
7.
8.
9.
10.

Action= None      Select Rule= N/A
Press ENTER to Confirm or ESC to Cancel:

```

Now configure the IGA3 to map to our web server and mail server on the LAN.

- 1** Enter 15 from the main menu.
- 2** Enter 2 in **Menu 15 - NAT Setup**.
- 3** Enter 1 in **Menu 15.2 - NAT Server Setup** to see the following menu. Configure it as shown.

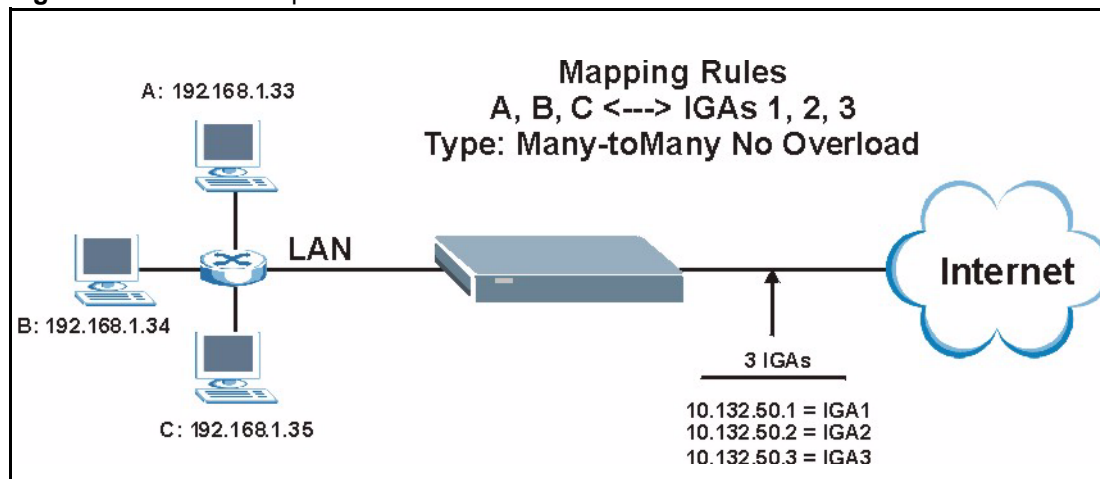
Figure 163 Example 3: Menu 15.2

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.21
3.	25	25	192.168.1.20
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:
 HTTP:80 FTP:21 Telnet:23 SMTP:25 POP3:110 PPTP:1723

28.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 164 NAT Example 4

Note: Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One and Many-to-Many No Overload mapping types.

Follow the steps outlined in example 3 to configure these two menus as follows

Figure 165 Example 4: Menu 15.1.1.1 Address Mapping Rule.

```

Menu 15.1.1.1 Address Mapping Rule

Type= Many-One-to-One
Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12
Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:
  
```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

Figure 166 Example 4: Menu 15.1.1 Address Mapping Rules

Menu 15.1.1 - Address Mapping Rules					
Set Name= Example4					
Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	192.168.1.10	192.168.1.12	10.132.50.1	10.132.50.3	M:M NO OV
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
Action= Edit Select Rule=					
Press ENTER to Confirm or ESC to Cancel:					

28.6 Configuring Trigger Port Forwarding



Note: Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.

Figure 167 Menu 15.3 Trigger Port Setup

Menu 15.3 - Trigger Port Setup					
Rule	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1.	Real Audio	6970	7170	7070	7070
2.		0	0	0	0
3.		0	0	0	0
4.		0	0	0	0
5.		0	0	0	0
6.		0	0	0	0
7.		0	0	0	0
8.		0	0	0	0
9.		0	0	0	0
10.		0	0	0	0
11.		0	0	0	0
12.		0	0	0	0
Press ENTER to Confirm or ESC to Cancel:					

The following table describes the fields in this screen.

Table 105 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION
Rule	This is the rule index number.
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyAIR forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyAIR to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 29

Filter Configuration

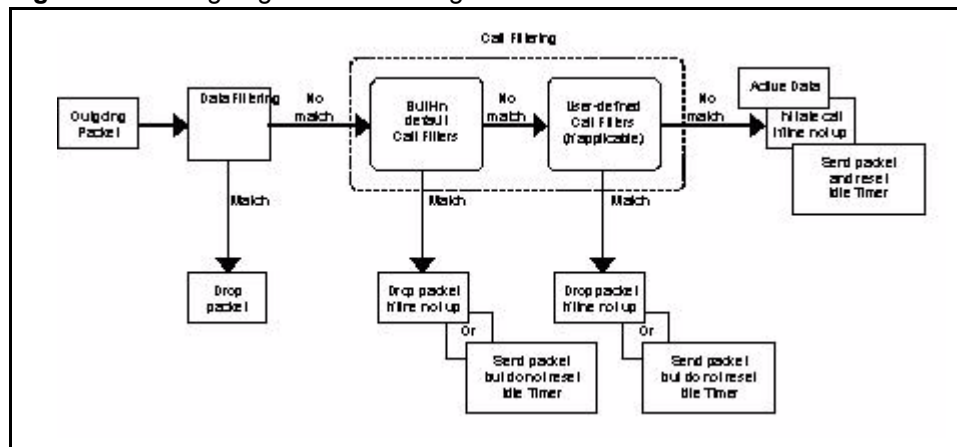
This chapter shows you how to create and apply filters.

29.1 Introduction to Filters

Your ZyAIR uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

Figure 168 Outgoing Packet Filtering Process



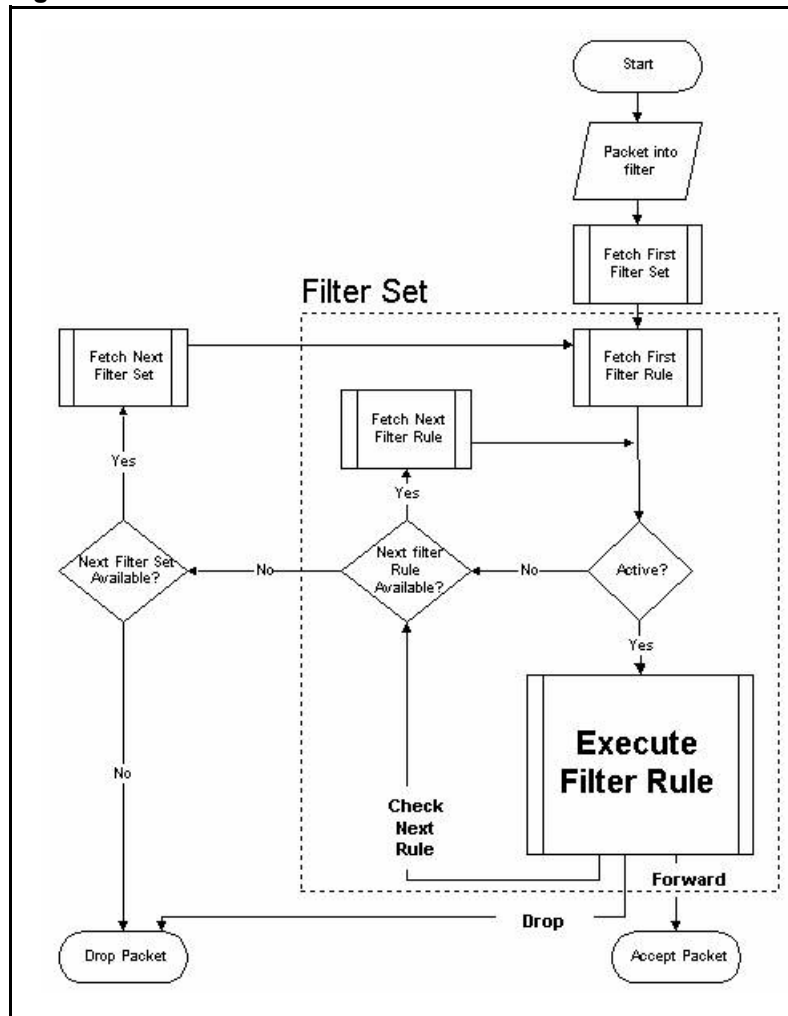
For incoming packets, your ZyAIR applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

29.1.1 The Filter Structure of the ZyAIR

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyAIR allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also [see Figure 173](#) for the logic flow when executing an IP filter.

Figure 169 Filter Rule Process

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

29.2 Configuring a Filter Set

The ZyAIR includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

- 1 Enter 21 in the main menu to open menu 21.

Figure 170 Menu 21: Filter and Firewall Setup

```

Menu 21 - Filter and Firewall Setup
    1. Filter Setup
    2. Firewall Setup

Enter Menu Selection Number:

```

2 Enter 1 to bring up the following menu.

Figure 171 Menu 21.1: Filter Set Configuration

```

Menu 21.1 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
1      _____      7      _____
2      _____      8      _____
3      _____      9      _____
4      _____     10      _____
5      _____     11      _____
6      _____     12      _____

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Select the filter set you wish to configure (1-12) and press [ENTER].

Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 106 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.

Table 106 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.
n	Action Not Matched “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 107 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	Protocol Source Address Source Port number Destination Address Destination Port number
Pr	
SA	
SP	
DA	
DP	
GEN	Offset Length
Off	
Len	

Refer to the next section for information on configuring the filter rules.

29.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyAIR will warn you and will not allow you to save.

29.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next

Figure 172 Menu 21.1.1.1 TCP/IP Filter Rule.

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr=
               IP Mask=
               Port #=
               Port # Comp= None
Source: IP Addr=
         IP Mask=
         Port #=
         Port # Comp= None
TCP Estab= N/A
More= No      Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

The following table describes how to configure your TCP/IP filter rule.

Table 108 TCP/IP Filter Rule

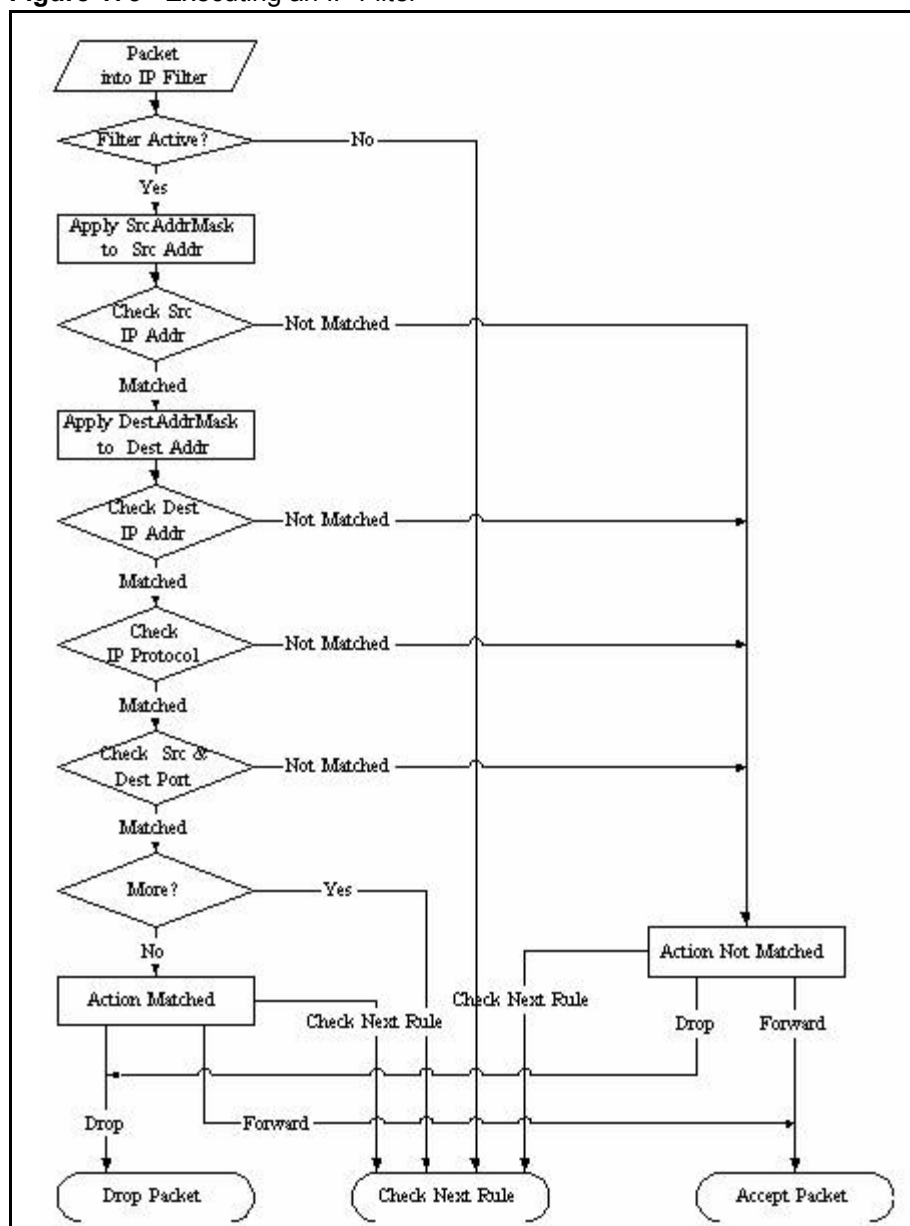
FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate the filter rule or No to deactivate it.	Yes No
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	Press [SPACE BAR] and then [ENTER] to select Yes to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.	Yes No
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the Destination: IP Addr.	0.0.0.0

Table 108 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in Destination: Port # .	None Less Greater Equal Not Equal
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the Source: IP Addr.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in Source: Port # .	None Less Greater Equal Not Equal
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select Yes , to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if No , it is ignored.	Yes No
More	Press [SPACE BAR] and then [ENTER] to select Yes or No . If Yes , a matching packet is passed to the next filter rule before an action is taken; if No , the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A .	Yes No
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: None – No packets will be logged. Action Matched - Only packets that match the rule parameters will be logged. Action Not Matched - Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	Check Next Rule Forward Drop
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	Check Next Rule Forward Drop
When you have Menu 21.1.1.1 - TCP/IP Filter Rule configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on Menu 21.1.1 - Filter Rules Summary .		

The following figure illustrates the logic flow of an IP filter.

Figure 173 Executing an IP Filter



29.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyAIR treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyAIR applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.

Figure 174 Menu 21.1.4.1 Generic Filter Rule

```

Menu 21.1.4.1 - Generic Filter Rule

Filter #: 4,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

The following table describes the fields in the Generic Filter Rule menu.

Table 109 Generic Filter Rule Menu Fields

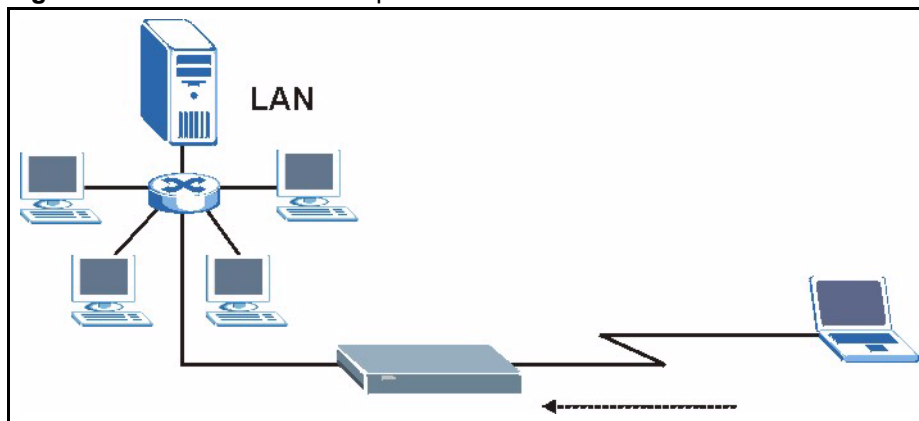
FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	Generic Filter Rule TCP/IP Filter Rule
Active	Select Yes to turn on the filter rule or No to turn it off.	Yes / No
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0-255
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0-8
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	

Table 109 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
More	If Yes , a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be No .	Yes No
Log	Select the logging option from the following: None - No packets will be logged. Action Matched - Only packets that match the rule parameters will be logged. Action Not Matched - Only packets that do not match the rule parameters will be logged. Both - All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Select the action for a packet matching the rule.	Check Next Rule Forward Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule Forward Drop
Once you have completed filling in Menu 21.4.1.1 - Generic Filter Rule , press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on Menu 21.1.1 - Filter Rules Summary .		

29.3 Example Filter

Let's look at an example to block outside users from accessing the ZyAIR via telnet.

Figure 175 Telnet Filter Example

- 1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- 2 Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- 3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- 4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

- 5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**
- 6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 176 Example Filter: Menu 21.1.3.1

```

Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port # = 23
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port # = 0
                Port # Comp= None
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

- Select **Yes** from the **Active** field to activate this rule.
- **6** is the TCP IP **Protocol**.
- The **Port #** for the telnet service (TCP protocol) is 23. See RFC 1060 for port numbers of well-known services.
- Select **Equal** from the **Port # Comp** field as you are looking for packets going to port 23 only.
- Select **Drop** in the **Action Matched** field so that the packet will be dropped if its destination is the telnet port.
- Select **Forward** from the **Action Not Matched** field so that the packet will be forwarded if its destination is not the telnet port.
- Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Figure 177 Example Filter Rules Summary: Menu 21.1.3

Menu 21.1.3 - Filter Rules Summary						
#	A	Type	Filter Rules			M m n
-	-	-	-	-	-	-
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23			N D F
2	N					
3	N					
4	N					
5	N					
6	N					

Enter Filter Rule Number (1-6) to Configure:

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

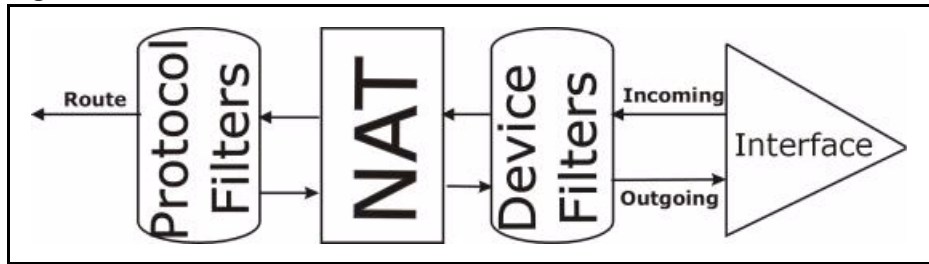
M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

After you've created the filter set, you must apply it.

- 1 Enter 11 from the main menu to go to menu 11.
- 2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
- 3 This brings you to menu 11.5. Apply a filter set (our example filter set 3).
- 4 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

29.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyAIR applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyAIR is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 178 Protocol and Device Filter Sets

29.5 Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

29.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The ZyAIR already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.



Note: If you do not activate the firewall, it is advisable to apply filters

29.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyAIR and output filter sets filter outgoing traffic from the ZyAIR. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 179 Filtering LAN Traffic

```
Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=

Output Filter Sets:
  protocol filters=
  device filters=

Press ENTER to Confirm or ESC to Cancel:
```

29.6.2 Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyAIR already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 180 Filtering Remote Node Traffic

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=

Output Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

CHAPTER 30

Enabling the Firewall

This chapter shows you how to get started with the ZyAIR firewall.

30.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

30.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyAIR has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

30.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter and Firewall Setup** to display the screen shown next.

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

Figure 181 Menu 21.2 Firewall Setup

```
Menu 21.2 - Firewall Setup

The firewall protects against Denial of Service (DoS) attacks when
it is active.

Your network is vulnerable to attacks when the firewall is turned off.

Refer to the User's Guide for details about the firewall default
policies.

You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so.

Active: Yes

You can use the Web Configurator to configure the firewall.

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```



Note: Use the web configurator or the command interpreter to configure the firewall rules.

CHAPTER 31

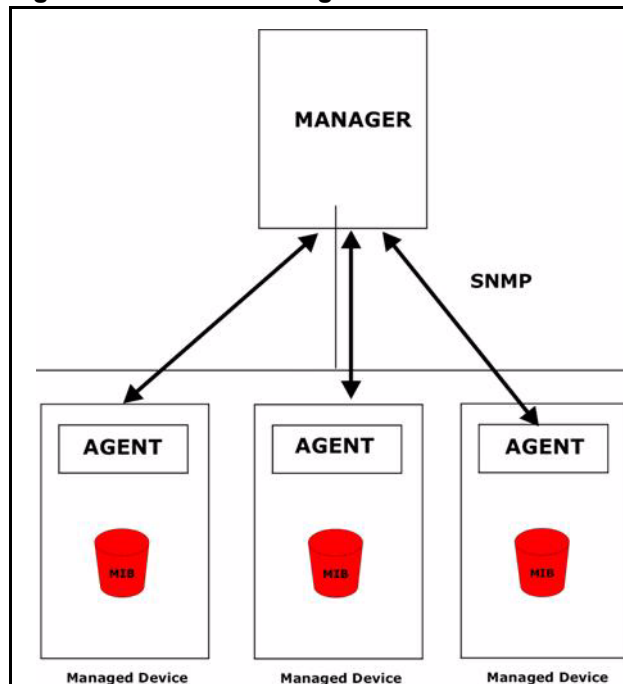
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

31.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 182 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyAIR). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include the number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

31.2 Supported MIBs

The ZyAIR supports RFC-1215 and MIB II as defined in RFC-1213. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

31.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 – SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

Figure 183 Menu 22 SNMP Configuration

```

Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the SNMP configuration parameters.

Table 110 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the Set Community , which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your ZyAIR will only respond to SNMP messages from this address. A blank (default) field means your ZyAIR will respond to all SNMP messages it receives, regardless of source.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

31.4 SNMP Traps

The ZyAIR will send traps to the SNMP manager when any one of the following events occurs:

Table 111 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkUp (<i>defined in RFC-1215</i>)	A trap is sent when the port is up.

Table 111 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
4	authenticationFailure (<i>defined in RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (<i>defined in RFC-1215</i>)	A trap is sent when the port is down.

The following table maps the physical port and encapsulation to the interface type,

Table 112 Ports and Interface Types

PHYSICAL PORT/ENCAP	INTERFACE TYPE
WLAN	enif0
Ethernet port	enif0
WAN	enif1

CHAPTER 32

System Security

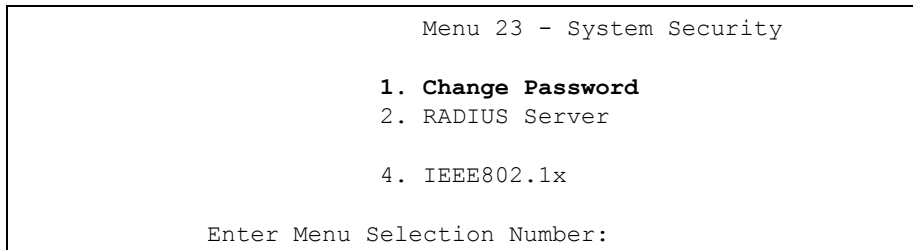
This chapter describes how to configure the system security on the ZyAIR.

32.1 System Security

You can configure the system password, an external RADIUS server and 802.1x in this menu.

32.1.1 System Password

Figure 184 Menu 23 System Security



The screenshot shows a terminal window titled "Menu 23 - System Security". Inside the window, there is a list of four options: "1. Change Password", "2. RADIUS Server", "3. (blank)", and "4. IEEE802.1x". At the bottom of the window, it says "Enter Menu Selection Number:". The options are numbered 1 through 4, with option 3 being blank.

```
Menu 23 - System Security

1. Change Password
2. RADIUS Server
3.
4. IEEE802.1x

Enter Menu Selection Number:
```

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the *Introducing the SMT* chapter and the section on resetting the ZyAIR in the *Introducing the Web Configurator* chapter.

32.1.2 Configuring External RADIUS Server

Enter 23 in the main menu to display **Menu 23 – System Security**.

Figure 185 Menu 23 System Security

```

Menu 23 - System Security

1. Change Password
2. RADIUS Server

4. IEEE802.1x

Enter Menu Selection Number:

```

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 – System Security – RADIUS Server** as shown next.

Figure 186 Menu 23.2 System Security : RADIUS Server

```

Menu 23.2 - System Security - RADIUS Server

Authentication Server:
  Active= No
  Server Address= 0.0.0.0
  Port #= 1812
  Shared Secret= *****

Accounting Server:
  Active= No
  Server Address= 0.0.0.0
  Port #= 1813
  Shared Secret= *****

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

Table 113 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION
Authentication Server	
Active	Press [SPACE BAR] to select Yes and press [ENTER] to enable user authentication through an external authentication server.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyAIR.
Accounting Server	

Table 113 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select Yes and press [ENTER] to enable user authentication through an external accounting server.
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port	The default port of the RADIUS server for accounting is 1813 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and ZyAIR.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

32.1.3 802.1x

The IEEE 802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

Follow the steps below to enable EAP authentication on your ZyAIR.

- 1 From the main menu, enter 23 to display **Menu23 – System Security**.

Figure 187 Menu 23 System Security

Menu 23 - System Security
1. Change Password
2. RADIUS Server
4. IEEE802.1x
Enter Menu Selection Number:

- 2 Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.

Figure 188 Menu 23.4 System Security : IEEE802.1x

```

Menu 23.4 - System Security - IEEE802.1x

Wireless Port Control= Authentication Required
ReAuthentication Timer (in second)= 1800
Idle Timeout (in second)= 3600

Key Management Protocol= 802.1x
Dynamic WEP Key Exchange= 128-bit WEP
PSK = N/A
WPA Mixed Mode= N/A

WPA Broadcast/Multicast Key Update Timer= N/A

Authentication Databases= RADIUS Only

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

Table 114 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	<p>Press [SPACE BAR] and select a security mode for the wireless LAN access. Select No Authentication Required to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.</p> <p>Selecting Authentication Required means wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p>Select No Access Allowed to block all wireless stations access to the wired network.</p> <p>The following fields are not available when you select No Authentication Required or No Access Allowed.</p>
ReAuthentication Timer (in second)	<p>Specify how often a client has to re-enter username and password to stay connected to the wired network.</p> <p>This field is activated only when you select Authentication Required in the Wireless Port Control field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is 1800 seconds (or 30 minutes).</p>
Idle Timeout (in second)	<p>The ZyAIR automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed.</p> <p>This field is activated only when you select Authentication Required in the Wireless Port Control field. The default time interval is 3600 seconds (or 1 hour).</p>
Key Management Protocol	<p>Press [SPACE BAR] to select 802.1x, WPA or WPA-PSK and press [ENTER].</p>

Table 114 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Dynamic WEP Key Exchange	<p>This field is activated only when you select Authentication Required in the Wireless Port Control field. Also set the Authentication Databases field to RADIUS Only. Local user database may not be used.</p> <p>Select Disable to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.</p> <p>Select 64-bit WEP or 128-bit WEP to enable data encryption.</p> <p>Up to 32 stations can access the ZyAIR when you configure Dynamic WEP Key Exchange.</p>
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select WPA-PSK in the Key Management Protocol field.
WPA Mixed Mode	Select Enable to activate WPA mixed mode. Otherwise, select Disable and configure Data Privacy for Broadcast/Multicast packets field.
WPA Group Key Update Timer	The WPA Broadcast/Multicast Key Update Timer is the rate at which the AP (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the WPA Broadcast/Multicast Key Update Timer is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).
Authentication Databases	<p>The authentication database contains wireless station login information. The RADIUS is an external server.</p> <p>When you configure Key Management Protocol to WPA, the Authentication Databases must be RADIUS Only.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the ZyAIR for authentication

CHAPTER 33

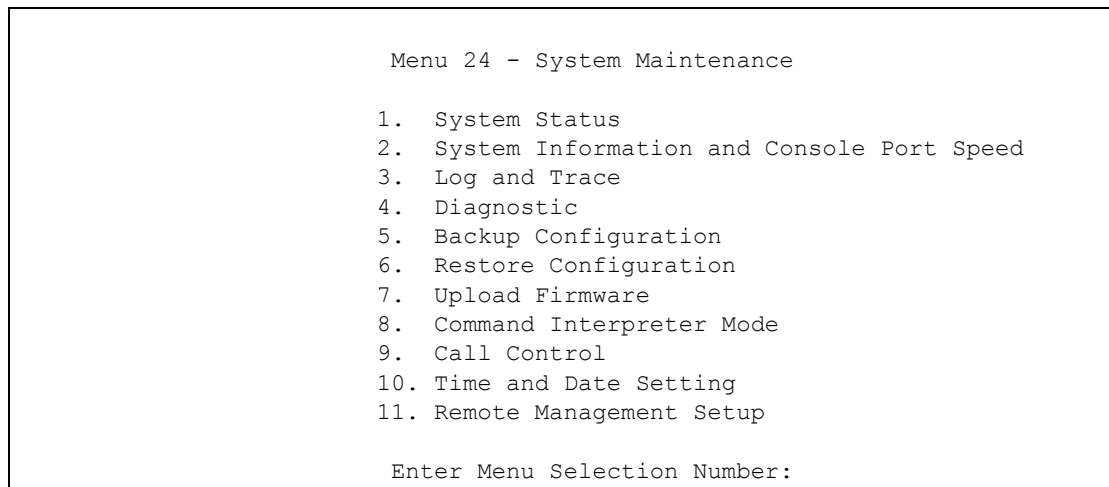
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu and press [ENTER] to open **Menu 24 – System Maintenance**, as shown in the following figure.

Figure 189 Menu 24 System Maintenance



33.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your ZyAIR. Specifically, it gives you information on your Ethernet and Wireless LAN status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 – System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 – System Maintenance – Status**. Entering 9 resets the counters; pressing [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are read-only and meant for diagnostic purposes.

Figure 190 Menu 24.1 System Maintenance : Status

Menu 24.1 - System Maintenance - Status					00:55:58		
					Sat. Jan. 01, 2000		
Port	Status	TxPkts	RxPkts	Cols	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	0:00:00
LAN	100M/Full	193	0	0	0	0	0:55:56
WLAN	54M	45	272	0	0	0	0:55:56
Port	Ethernet Address		IP Address		IP Mask		DHCP
WAN	00:A0:C5:9C:40:1D		0.0.0.0		0.0.0.0		Client
LAN	00:A0:C5:9C:40:1C		192.168.1.1		255.255.255.0		Server
WLAN	00:A0:C5:9C:40:1C						
System up Time:		0:56:02					
Name: G-2000PLUS							
Routing: IP							
ZyNOS F/W Version: V3.60(HU.0)b4 11/16/2004							
Press Command:							
COMMANDS: 1-Drop WAN 9-Reset Counters ESC-Exit							

The following table describes the fields present in this menu.

Table 115 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
Port	This is the port type. Port types are: Ethernet and Wireless
Status	This shows the status of the remote node.
TxPkts	This is the number of transmitted packets to this remote node.
RxPkts	This is the number of received packets from this remote node.
Cols	This is the number of collisions on this connection.
Tx B/s	This shows the transmission rate in bytes per second.
Rx B/s	This shows the receiving rate in bytes per second.
Up Time	This is the time this channel has been connected to the current remote node.
Ethernet Address	This shows the MAC address of the port.
IP Address	This shows the IP address of the network device connected to the port.
IP Mask	This shows the subnet mask of the network device connected to the port.
DHCP	This shows the DHCP setting (None or Client) for the port.
System Up Time	This is the time the ZyAIR is up and running from the last reboot.
Name	This displays the device name.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.

33.2 System Information

To get to the System Information:

- 1 Enter 24 to display **Menu 24 – System Maintenance**.
- 2 Enter 2 to display **Menu 24.2 – System Information and Console Port Speed**.
- 3 From this menu you have two choices as shown in the next figure:

Figure 191 Menu 24.2 System Information and Console Port Speed

```
Menu 24.2 - System Information and Console Port Speed

1. System Information
2. Console Port Speed
```



Note: The ZyAIR also has an internal console port for support personnel only. Do not open the ZyAIR as it will void your warranty.

33.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

Figure 192 Menu 24.2.1 System Information : Information

```
Menu 24.2.1 - System Maintenance - Information

Name: G-2000PLUS
Routing: IP
ZyNOS F/W Version: V3.60(HU.0)b4 | 11/16/2004
Country Code: 255

LAN
Ethernet Address: 00:A0:C5:9C:40:1C
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

Table 116 Menu 24.2.1 System Maintenance : Information

FIELD	DESCRIPTION
Name	Displays the system name of your ZyAIR. This information can be changed in Menu 1 – General Setup .
Routing	Refers to the routing protocol used.

Table 116 Menu 24.2.1 System Maintenance : Information

FIELD	DESCRIPTION
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your ZyAIR.
IP Address	This is the IP address of the ZyAIR in dotted decimal notation.
IP Mask	This shows the subnet mask of the ZyAIR.
DHCP	This field shows the DHCP setting of the ZyAIR.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

33.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your ZyAIR supports 9600 (default), 19200, 38400, 57600 and 115200 bps console port speeds. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

Figure 193 Menu 24.2.2 System Maintenance : Change Console Port Speed

```

Menu 24.2.2 - System Maintenance - Change Console Port Speed

      Console Port Speed: 9600

Press ENTER to Confirm or ESC to Cancel:

```

After you changed the console port speed on your ZyAIR, you must also make the same change to the console port speed parameter of your communication software.

33.3 Log and Trace

Your ZyAIR provides the error logs and trace records that are stored locally.

33.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

- 1 Type 24 in the main menu to display **Menu 24 – System Maintenance**.
- 2 From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

Figure 194 Menu 24.3 System Maintenance : Log and Trace

```

Menu 24.3 - System Maintenance - Log and Trace

2. Syslog Logging

4. Call-Triggering Packet

```

33.3.2 UNIX Syslog

The ZyAIR uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog can be configured in **Menu 24.3.2 – System Maintenance – UNIX Syslog**, as shown next.

Figure 195 Menu 24.3.2 System Maintenance : UNIX Syslog

```

Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:
Active= No
Syslog Server IP Address= 0.0.0.0
Log Facility= Local 1

```

You need to configure the UNIX syslog parameters described in the following table to activate syslog and then choose what you want to log.

Table 117 Menu 24.3.2 System Maintenance : UNIX Syslog

PARAMETER	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog logging on or off.
Syslog Server IP Address	Type the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a location. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Your ZyAIR sends five types of syslog messages. Some examples (not all ZyAIR specific) of these syslog messages with their message formats are shown next:

33.3.2.1 CDR

```
SdcmdSyslogSend ( SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new
call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxxx (L2TP, xxxxxx = Remote Call ID)
C01 Incoming Call xxxx (= connected speed) xxxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxx (= connected speed) xxxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated
```

33.3.2.2 Packet triggered

```
Packet triggered Message Format
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx....x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

33.3.2.3 Filter log

```

Filter log Message Format
SdcmSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match
(m) drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[fffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[fffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

```

33.3.2.4 PPP log

```

PPP Log Message Format
SdcmSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing

```

33.3.2.5 Firewall log

```
Firewall Log Message Format
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol ("TCP", "UDP", "ICMP", "IGMP", "GRE", "ESP")
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-200011:48:41Local11.Notice192.168.10.10RAS: FW 172.21.1.80      :137  -
>172.21.1.80      :137  |UDP|default permit:<2,0>|B
08-01-200011:48:41Local11.Notice192.168.10.10RAS: FW 192.168.77.88  :520  -
>192.168.77.88   :520  |UDP|default permit:<2,0>|B
08-01-200011:48:39Local11.Notice192.168.10.10RAS: FW 172.21.1.50    ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-200011:48:39Local11.Notice192.168.10.10RAS: FW 172.21.1.25    ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

33.3.3 Call-Triggering Packet

Call-triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hexadecimal format.

Figure 196 Call-Triggering Packet Example

```

IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
Frame Type:
  IP Header:
    IP Version           = 4
    Header Length        = 20
    Type of Service      = 0x00 (0)
    Total Length         = 0x002C (44)
    Identification      = 0x0002 (2)
    Flags                = 0x00
    Fragment Offset      = 0x00
    Time to Live         = 0xFE (254)
    Protocol             = 0x06 (TCP)
    Header Checksum      = 0xFB20 (64288)
    Source IP           = 0xC0A80101 (192.168.1.1)
    Destination IP      = 0x00000000 (0.0.0.0)
  TCP Header:
    Source Port          = 0x0401 (1025)
    Destination Port     = 0x000D (13)
    Sequence Number      = 0x05B8D000 (95997952)
    Ack Number           = 0x00000000 (0)
    Header Length        = 24
    Flags                = 0x02 (....S.)
    Window Size          = 0x2000 (8192)
    Checksum             = 0xE06A (57450)
    Urgent Ptr           = 0x0000 (0)
    Options              =
                        0000: 02 04 02 00
  RAW DATA:
    0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.....
    0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  .....
    0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...

```

33.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyAIR to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to display this menu:

- 1** From the main menu, type 24 to open **Menu 24 – System Maintenance**.

- 2 From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

```

Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
  1. Ping Host
  2. WAN DHCP Release
  3. WAN DHCP Renewal
  4. Internet Setup Test

System
  11. Reboot System

Enter Menu Selection Number:

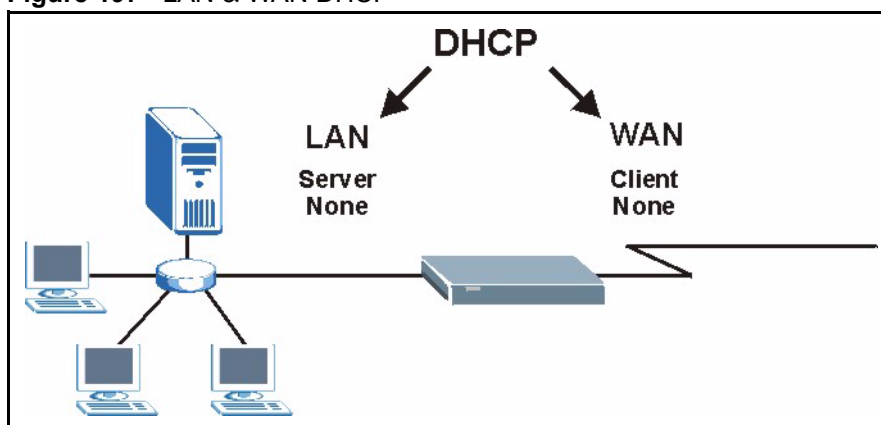
Host IP Address= N/A

```

33.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in LAN & WAN DHCP. LAN DHCP has already been discussed. The ZyAIR can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

Figure 197 LAN & WAN DHCP



The following table describes the diagnostic tests available in menu 24.4 for your ZyAIR and associated connections..

Table 118 Menu 24.4 System Maintenance Menu: Diagnostic

FIELD	DESCRIPTION
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
WAN DHCP Release	Release the IP address assigned by the DHCP server.

Table 118 Menu 24.4 System Maintenance Menu: Diagnostic

FIELD	DESCRIPTION
WAN DHCP Renewal	Get a new IP address from the DHCP server.
Reboot System	Reboot the ZyAIR.
Host IP Address	If you typed 1 to Ping Host, now type the address of the computer you want to ping.

CHAPTER 34

Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files using the SMT screens.

34.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a rom filename extension. Once you have customized the ZyAIR's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyAIR.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file config.cfg.

If your [T]FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyAIR only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyAIR and the external filename refers to the filename not on the ZyAIR, that is, on your computer, local network or FTP site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version.

Table 119 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the ZyAIR. Uploading the rom-0 file replaces the entire ROM file system, including your ZyAIR configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the ZyAIR.

34.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyAIR configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms “download” and “upload” are relative to the computer. Download means to transfer from the ZyAIR to the computer, while upload means from your computer to the ZyAIR.

34.2.1 Backup Configuration Using FTP

Enter 5 in **Menu 24 – System Maintenance** to get the following screen.

Figure 198 Menu 24.5 Backup Configuration**Menu 24.5 - Backup Configuration**

To transfer the configuration file to your workstation, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to your workstation.

For details on FTP commands, please consult the documentation of your FTP client program. For details on backup using TFTP (note that you must remain in the menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:

34.2.2 Using the FTP command from the DOS Prompt

- 1 Launch the FTP client on your computer.
- 2 Enter "open" and the IP address of your ZyAIR.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter "root" and your SMT password as requested. The default is 1234.
- 5 Enter "bin" to set transfer mode to binary.
- 6 Use "get" to transfer files from the ZyAIR to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the ZyAIR to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.
- 7 Enter "quit" to exit the FTP prompt.

Figure 199 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

34.2.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in third party FTP clients.

Table 120 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

34.2.4 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- 1 You have disabled Telnet service in menu 24.11.
- 2 You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- 3 The IP address in the Secured Client IP field in menu 24.11 does not match the client IP. If it does not match, the ZyAIR will disconnect the Telnet session immediately.
- 4 You have an SMT console session running.

34.2.5 Backup Configuration Using TFTP

The ZyAIR supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next:

- 1 Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the configuration file is `rom-0` (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyAIR to the computer and “binary” to set binary transfer mode.

34.2.6 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyAIR IP address, “get” transfers the file source on the ZyAIR (rom-0 name of the configuration file on the ZyAIR) to the file destination on the computer and renames it `config.rom`.

34.2.7 GUI-based TFTP Clients

The following table describes some of the fields that you may see in third party TFTP clients.

Table 121 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyAIR. 192.168.1.2 is the ZyAIR's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyAIR and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyAIR. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

34.3 Restore Configuration

Menu 24.6 — System Maintenance – Restore Configuration allows you to restore the configuration via FTP or TFTP to your ZyAIR. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The ZyAIR restarts automatically after the file transfer is complete.

34.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 200 Menu 24.6 Restore Configuration

```

Menu 24.6 - Restore Configuration
To transfer the firmware and the configuration file, follow the procedure
below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-spt is the
   Remote file name on the router. This restores the configuration to your
   router.
4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring using TFTP (note that you must
remain in the menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:

```

- 1** Launch the FTP client on your computer.
- 2** Enter "open", followed by a space and the IP address of your ZyAIR.
- 3** Press [ENTER] when prompted for a username.
- 4** Enter your password as requested (the default is "1234").
- 5** Enter "bin" to set transfer mode to binary.
- 6** Find the "rom" file (on your computer) that you want to restore to your ZyAIR.
- 7** Use "put" to transfer files from the ZyAIR to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the ZyAIR. See earlier in this chapter for more information on filename conventions.
- 8** Enter "quit" to exit the ftp prompt. The ZyAIR will automatically restart after a successful restore process.

34.3.2 Restore Using FTP Session Example

Figure 201 Restore Using FTP Session Example

```

ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit

```

Refer to section [34.2.4](#) to read about configurations that disallow TFTP and FTP over WAN.

34.4 Uploading Firmware and Configuration Files

Menu 24.7 – System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file.



Note: WARNING! PLEASE WAIT A FEW MINUTES FOR THE ZYAIR TO RESTART AFTER FIRMWARE OR CONFIGURATION FILE UPLOAD. INTERRUPTING THE UPLOAD PROCESS MAY PERMANENTLY DAMAGE YOUR ZYAIR.

Figure 202 Menu 24.7 System Maintenance: Upload Firmware

<pre>Menu 24.7 - System Maintenance - Upload Firmware 1. Upload System Firmware 2. Upload System Configuration File Enter Menu Selection Number:</pre>
--

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

34.4.1 Firmware Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyAIR, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 203 Menu 24.7.1 System Maintenance : Upload System Firmware

```

Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name of your
   firmware upgrade file on your workstation and "ras" is the remote file name on the
   system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP), please see
your manual.

Press ENTER to Exit:

```

34.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 204 Menu 24.7.2 System Maintenance: Upload System Configuration File

```

Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and SMT   password
   as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename" is the name of
   your system configuration file on your workstation, which will be transferred to the
   "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration file process
   is complete.

For details on FTP commands, please consult the documentation of your FTP client
program. For details on uploading system firmware using TFTP (note that you must
remain on this menu to upload system firmware using TFTP), please see your manual.

Press ENTER to Exit:

```

To transfer the firmware and the configuration file, follow these examples:

34.4.3 Using the FTP command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter "open" and the IP address of your ZyAIR.
- 3 Press [ENTER] when prompted for a username.

- 4 Enter “root” and your SMT password as requested. The default is 1234.
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the ZyAIR, e.g., put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the ZyAIR and renames it “ras”. Similarly “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyAIR and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyAIR to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the FTP prompt.

Figure 205 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

More commands that you may find in third party FTP clients are listed earlier in this chapter.

34.4.4 TFTP File Upload

The ZyAIR also supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next:

- 1 Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter the command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.

- 5 Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the firmware is “ras” and the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyAIR to the computer, “put” the other way around, and “binary” to set binary transfer mode.

34.4.5 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyAIR’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyAIR).

Commands that you may see in third party TFTP clients are listed earlier in this chapter.

CHAPTER 35

System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

35.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 – System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

Figure 206 Menu 24 System Maintenance

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

Figure 207 Valid CI Commands

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
G-2000PLU> ?
Valid commands are:
sys                exit                device                ether
poe                pptp                config                wlan
ip                 ppp                bridge                certificates
radius            8021x                radserv
G-2000PLU>
```

35.2 Call Control Support

The ZyAIR provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyAIR within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

Figure 208 Menu 24.9 System Maintenance : Call Control

```

Menu 24.9 - System Maintenance - Call Control

1. Budget Management
2. Call History

Enter Menu Selection Number:

```

35.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 209 Budget Management

```

Menu 24.9.3 - Budget Management

Remote Node      Connection Time/Total Budget      Elapsed Time/Total Period
1.ChangeMe              No Budget                      No Budget

Reset Node (0 to update screen):

```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 122 Menu 24.9.1 - Budget Management

FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.
Enter "0" to update the screen or press [ESC] to return to the previous screen.	

35.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 210 Menu 24.9.2 - Call History

Menu 24.9.4 - Call History						
Phone Number	Dir	Rate	#call	Max	Min	Total
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Enter Entry to Delete(0 to exit):

The following table describes the fields in this menu.

Table 123 Call History Fields

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or "0" to exit.	

35.3 Time and Date Setting

The ZyAIR keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyAIR. Menu 24.10 allows you to update the time and date settings of your ZyAIR. The real time is then displayed in the ZyAIR error logs.

- 1 Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.
- 2 Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your ZyAIR as shown in the following screen.

Figure 211 Menu 24.10 System Maintenance : Time and Date Setting

```

Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= Manual
Time Server Address= N/A

Current Time:                01 : 00 : 37
New Time (hh:mm:ss):        01 : 00 : 34

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):          01 - 01
End Date (mm-dd):            01 - 01

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

The following table describes the fields in this menu.

Table 124 System Maintenance : Time and Date Setting

FIELD	DESCRIPTION
Time Protocol	Enter the time service protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC-1305) is similar to Time (RFC-868) . None. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/ network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose Yes .
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

35.3.1 Resetting the Time

The ZyAIR resets the time in three instances:

- 1** On leaving menu 24.10 after making changes.
- 2** When the ZyAIR starts up, if there is a timeserver configured in menu 24.10.
- 3** 24-hour intervals after starting.

CHAPTER 36

Remote Management

This chapter covers remote management (SMT menu 24.11).

36.1 Remote Management

Remote management allows you to determine which services/protocols can access which ZyAIR interface (if any) from which computers.

You may manage your ZyAIR from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable).



Note: When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

Figure 212 Menu 24.11 – Remote Management Control

Menu 24.11 - Remote Management Control		
TELNET Server:	Port = 23	Access = LAN only Secure Client IP = 0.0.0.0
FTP Server:	Port = 21	Access = LAN only Secure Client IP = 0.0.0.0
Web Server:	Port = 80	Access = LAN only Secure Client IP = 0.0.0.0
SNMP Service:	Port = 161	Access = LAN only Secure Client IP = 0.0.0.0
DNS Service:	Port = 53	Access = LAN only Secure Client IP = 0.0.0.0
Press ENTER to Confirm or ESC to Cancel:		

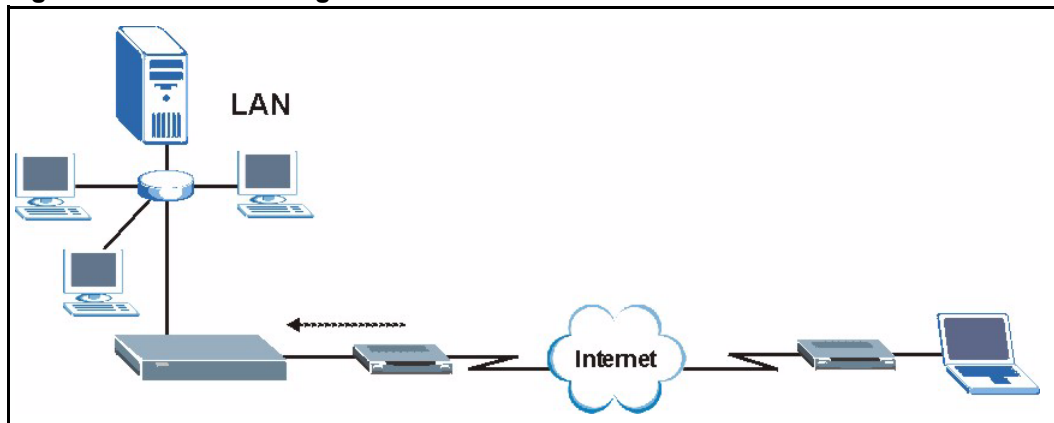
The following table describes the fields in this screen.

Table 125 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service or protocol.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyAIR.
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: LAN only , WAN only , ALL or Disable .
Secure Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the ZyAIR. Enter an IP address to restrict access to a client with a matching IP address.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

36.1.1 Telnet

You can configure your ZyAIR for remote Telnet access as shown next.

Figure 213 Telnet Configuration on a TCP/IP Network

36.1.2 FTP

You can upload and download ZyAIR firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

36.1.3 Web

You can use the ZyAIR's embedded web configurator for configuration and file management. See the Online Help for details.

36.1.4 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1** A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2** You have disabled that service in menu 24.11.
- 3** The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
- 4** There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
- 5** There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

36.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyAIR's WAN IP address when configuring from the WAN.
- Use the ZyAIR's LAN IP address when configuring from the LAN.

36.3 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your ZyAIR will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

CHAPTER 37

Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

37.1 Introduction to Call Scheduling

The call scheduling feature allows the ZyAIR to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

Figure 214 Menu 26 Schedule Setup

Menu 26 - Schedule Setup

Schedule Set #	Name	Schedule Set #	Name
1		7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Schedule Set Number to Configure=

Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the ZyAIR, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.



Note: To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

Figure 215 Menu 26.1 Schedule Set Setup

```

Menu 26.1 Schedule Set Setup

Active= Yes
Start Date(yyyy-mm-dd)= 2000 - 01 - 01
How Often= Once
Once:
    Date(yyyy-mm-dd)= 2000 - 01 - 01
Weekdays:
    Sunday= N/A
    Monday= N/A
    Tuesday= N/A
    Wednesday= N/A
    Thursday= N/A
    Friday= N/A
    Saturday= N/A
Start Time(hh:mm)= 00 : 00
Duration(hh:mm)= 00 : 00
Action= Forced On

                                Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

If a connection has been already established, your ZyAIR will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 126 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select Yes or No . Choose Yes and press [ENTER] to activate the schedule set.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select Once or Weekly . Both these options are mutually exclusive. If Once is selected, then all weekday settings are N/A . When Once is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once: Date	If you selected Once in the How Often field above, then enter the date the set should activate here in year-month-date format.
Weekday: Day	If you selected Weekly in the How Often field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select Yes , then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.

Table 126 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
Action	<p>Forced On means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the Duration field.</p> <p>Forced Down means that the connection is blocked whether or not there is a demand call on the line.</p> <p>Enable Dial-On-Demand means that this schedule permits a demand call on the line.</p> <p>Disable Dial-On-Demand means that this schedule prevents a demand call on the line.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

Figure 216 Applying Schedule Set(s) to a Remote Node (PPPoE)

```

Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP                      Route= IP
Active= Yes
Encapsulation= PPPoE                      Edit IP= No
Service Type= Standard                   Telco Option:
Service Name=                           Allocated Budget(min)= 0
Outgoing:                               Period(hr)= 0
My Login=                               Schedules= 1,2,3,4
My Password= *****                   Nailed-Up Connection= No
Retype to Confirm= *****
Authen= CHAP/PAP

Session Options:
Edit Filter Sets= No
Idle Timeout(sec)= 100
Edit Traffic Redirect= No

Press ENTER to Confirm or ESC to Cancel:

```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Appendix A

Troubleshooting

This appendix covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem.

Problems Starting Up the ZyAIR

Table 127 Troubleshooting the Start-Up of Your ZyAIR

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I plug in the power adaptor.	Make sure you are using the supplied power adaptor and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.
The ZyAIR reboots automatically sometimes.	The supplied power to the ZyAIR is too low. Check that the ZyAIR is receiving enough power. Make sure the power source is working properly.

Problems with the Ethernet Interface

Table 128 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyAIR from the LAN.	If the ETHN LED on the front panel is off, check the Ethernet cable connection between your ZyAIR and the Ethernet device connected to the ETHERNET port. Check for faulty Ethernet cables. Make sure your computer's Ethernet adapter is installed and working properly. Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the ZyAIR, the Ethernet device and your computer are on the same subnet.
I cannot ping any computer on the LAN.	If the ETHN LED on the front panel is off, check the Ethernet cable connections between your ZyAIR and the Ethernet device. Check the Ethernet cable connections between the Ethernet device and the LAN computers. Check for faulty Ethernet cables. Make sure the LAN computer's Ethernet adapter is installed and working properly. Verify that the IP address and the subnet mask of the ZyAIR, the Ethernet device and the LAN computers are on the same subnet.

Problems with the Password

Table 129 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR.	The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the RESET button on the top panel of the ZyAIR to restore the factory default configuration file (hold this button in for about 10 seconds or until the link LED turns red). This will restore all of the factory defaults including the password.

Problems with Telnet

Table 130 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR through Telnet.	Refer to the <i>Problems with the Ethernet Interface</i> section for instructions on checking your Ethernet connection.

Problems with the WLAN Interface

Table 131 Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyAIR from the WLAN.	Make sure the wireless card is properly inserted in the ZyAIR and the link LED is on. Make sure the wireless adapter on the wireless station is working properly. Check that both the ZyAIR and your wireless station are using the same ESSID, channel and WEP keys (if WEP encryption is activated).
I cannot ping any computer on the WLAN.	Make sure the wireless card is properly inserted in the ZyAIR and the link LED is on. Make sure the wireless adapter on the wireless station(s) is working properly. Check that both the ZyAIR and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Appendix B

Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See [Appendix F](#) for information on the command structure.

Table 132 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwdertrtm	This command displays the brute-force guessing password protection settings.
sys pwdertrtm 0	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwdertrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

```
sys pwdertrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

Appendix C

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

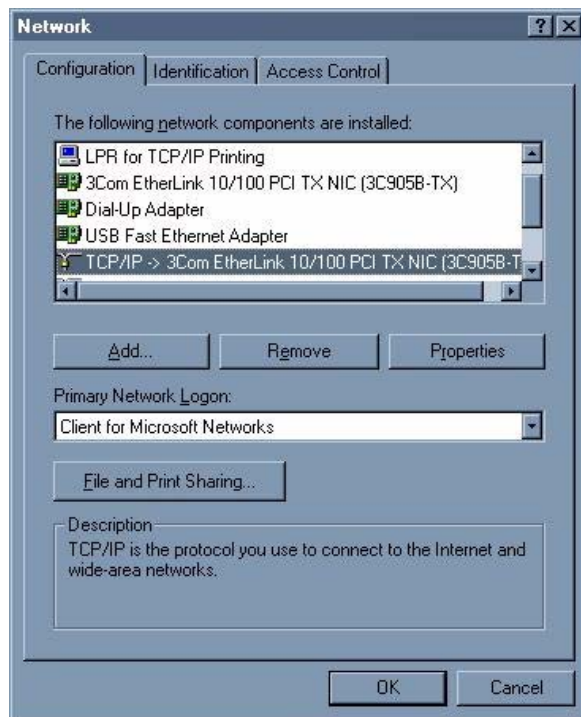
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyAIR's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 217 Windows 95/98/Me: Network: Configuration

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

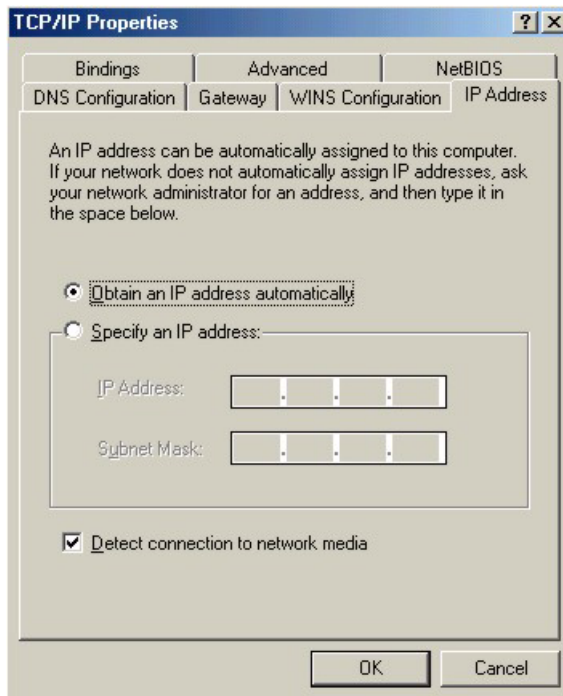
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

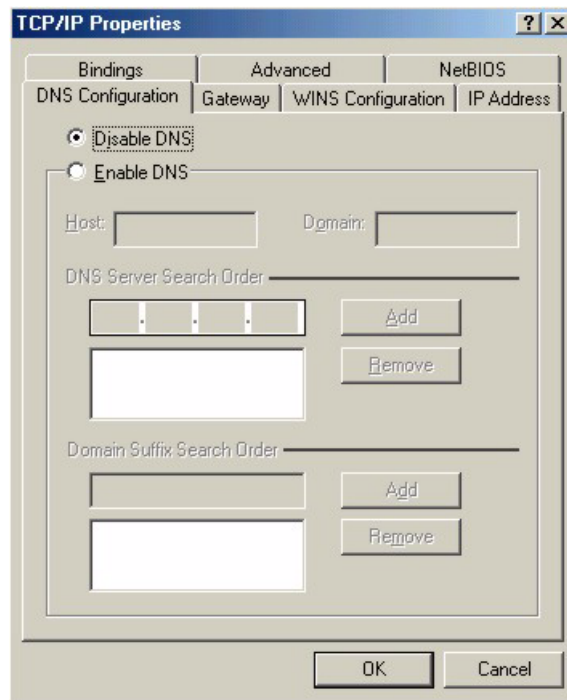
Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 218 Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
 - If you do not know your DNS information, select **Disable DNS**.
 - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 219 Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Turn on your ZyAIR and restart your computer when prompted.

Verifying Settings

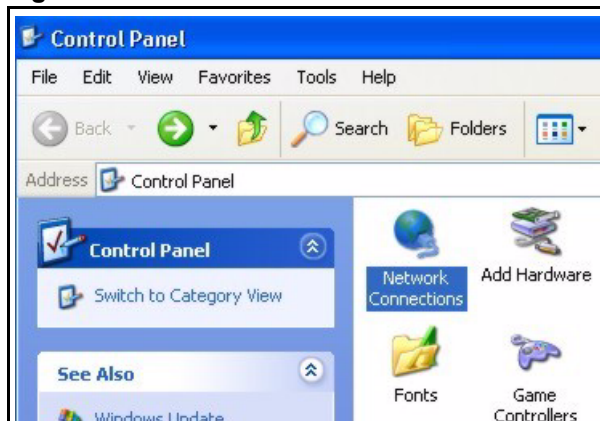
1 Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

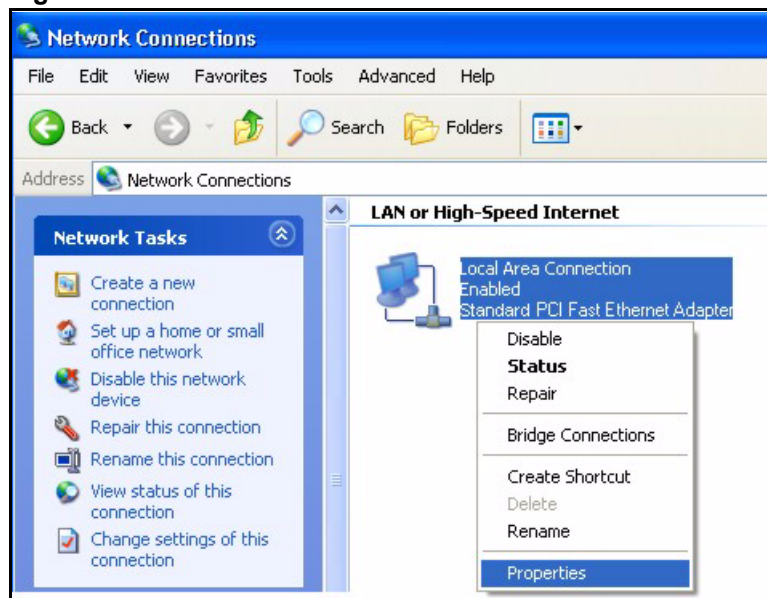
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 220 Windows XP: Start Menu

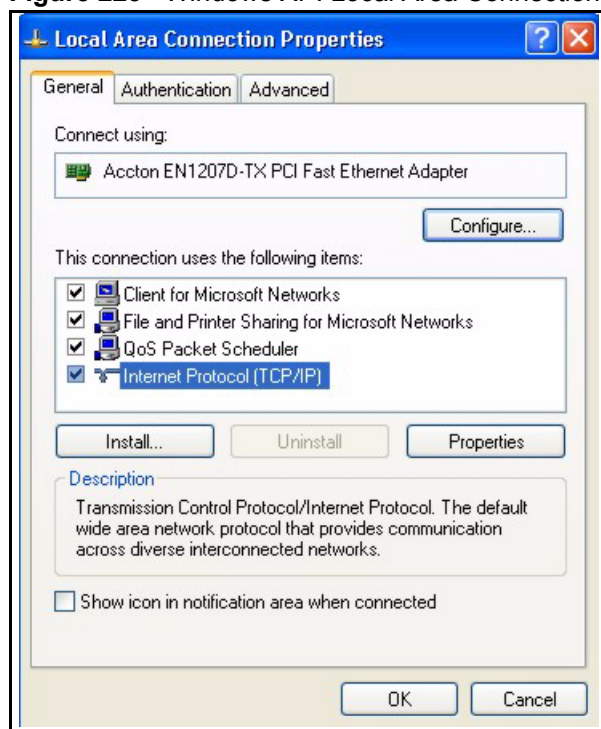
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 221 Windows XP: Control Panel

3 Right-click **Local Area Connection** and then click **Properties**.

Figure 222 Windows XP: Control Panel: Network Connections: Properties

- 4** Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

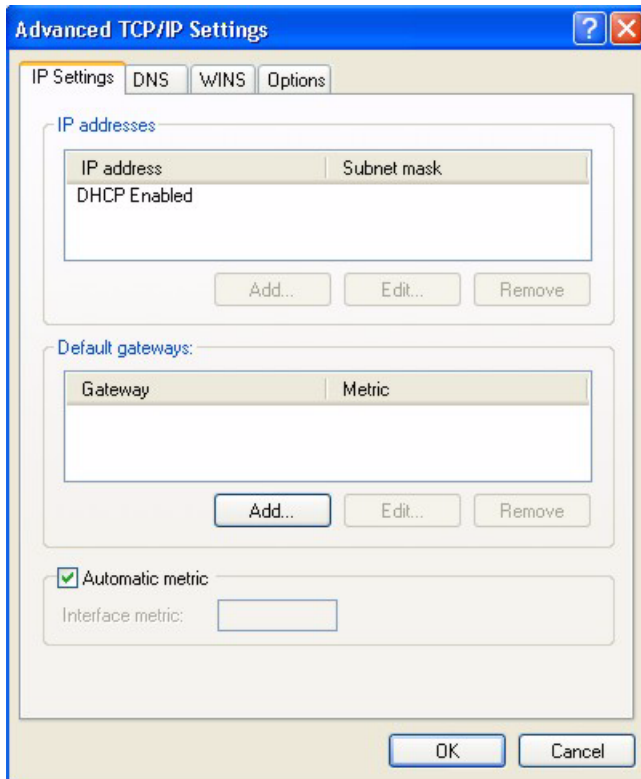
Figure 223 Windows XP: Local Area Connection Properties

- 5** The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 224 Windows XP: Advanced TCP/IP Settings



- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

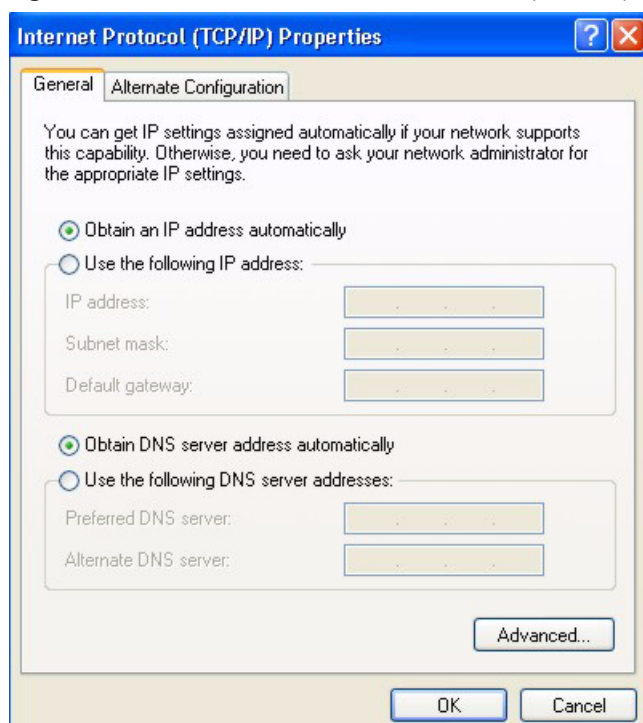
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 225 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

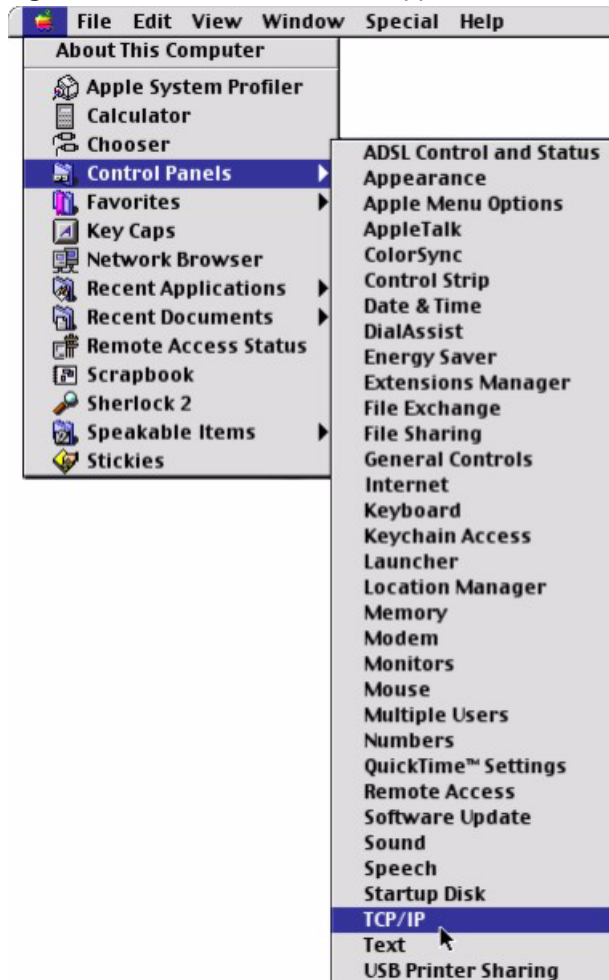
10 Turn on your ZyAIR and restart your computer (if prompted).

Verifying Settings

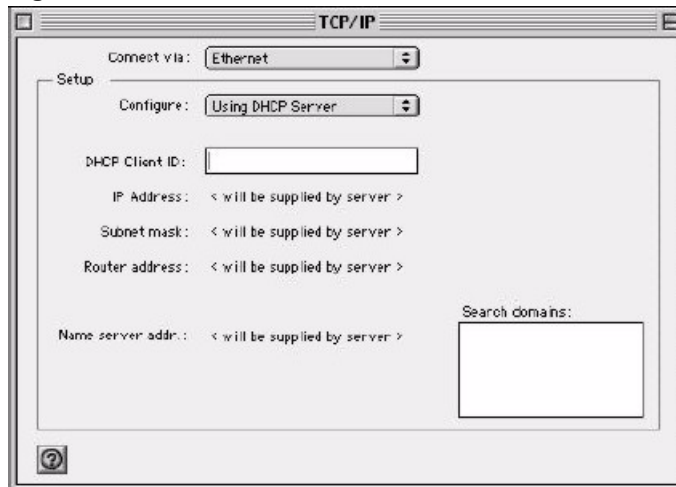
- 1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 226 Macintosh OS 8/9: Apple Menu

2 Select **Ethernet built-in** from the **Connect via** list.

Figure 227 Macintosh OS 8/9: TCP/IP

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

- 4 For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your ZyAIR in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your ZyAIR and restart your computer (if prompted).

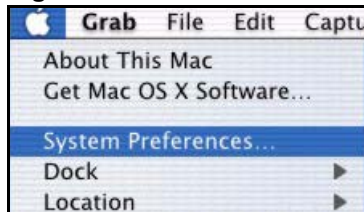
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

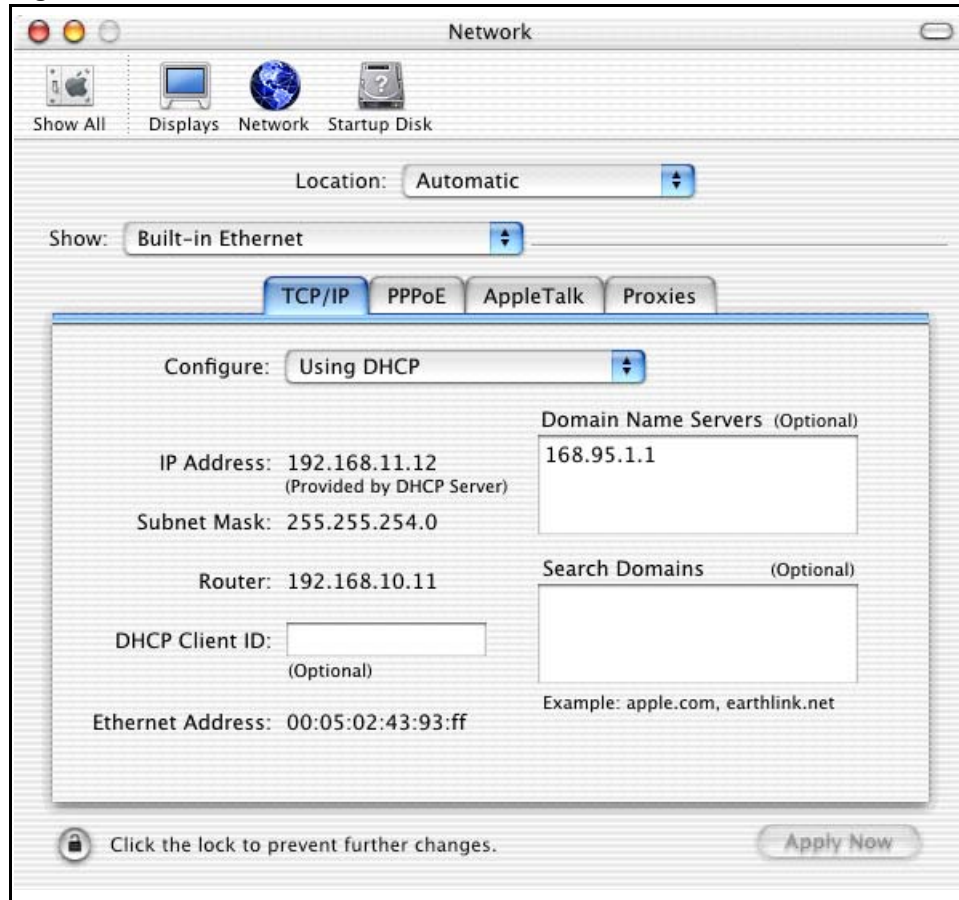
Macintosh OS X

- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 228 Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 229 Macintosh OS X: Network

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyAIR in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyAIR and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix D

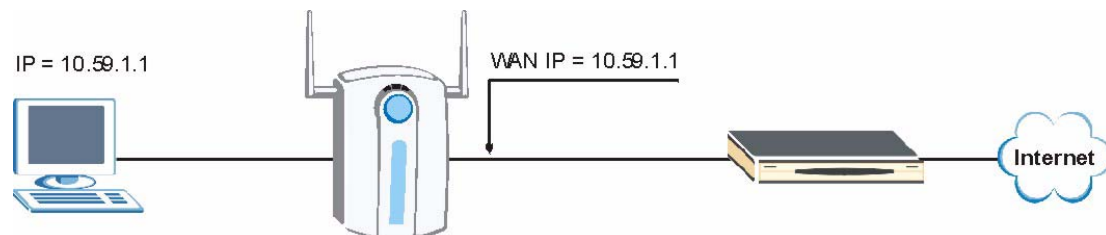
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Case A: The ZyAIR is using the same LAN and WAN IP addresses

The following figure shows an example where the ZyAIR is using a WAN IP address that is the same as the IP address of a computer on the LAN.

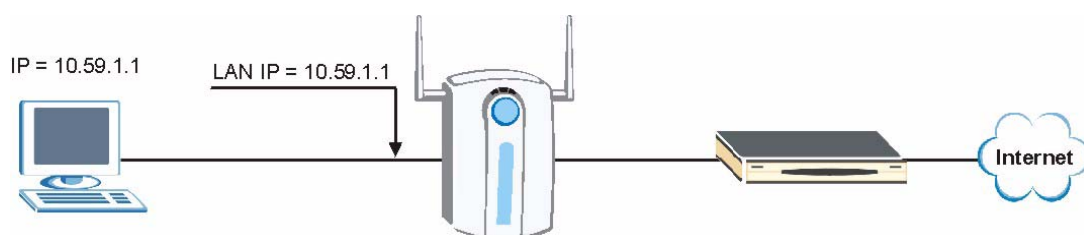
Figure 230 IP Address Conflicts: CaseA



You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

Case B: The ZyAIR LAN IP address conflicts with the DHCP client IP address

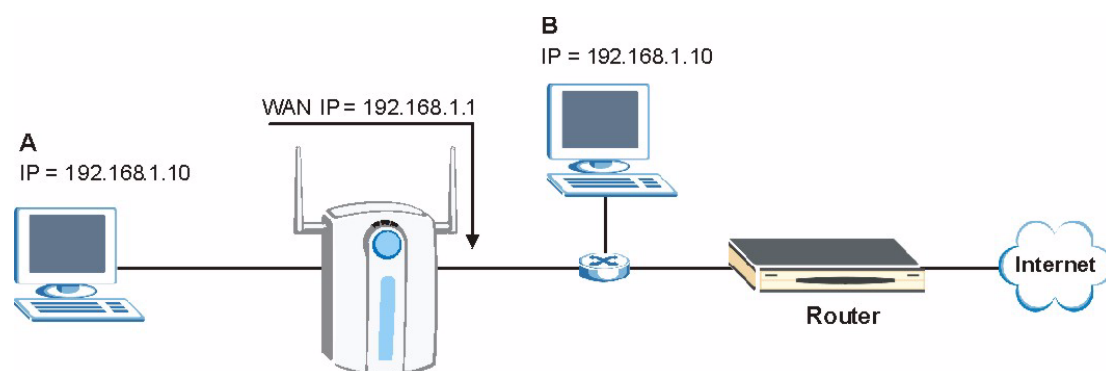
In the following figure, the ZyAIR is acting as a DHCP server. The ZyAIR assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

Figure 231 IP Address Conflicts: Case B

To solve this problem, make sure the ZyAIR LAN IP address is not in the DHCP IP address pool.

Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the ZyAIR.

Figure 232 IP Address Conflicts: Case C

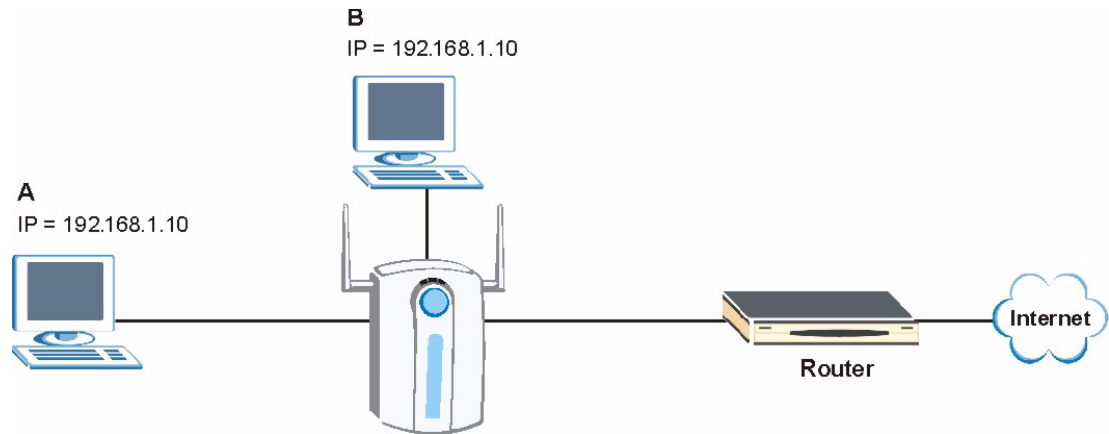
You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the ZyAIR allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the ZyAIR DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

Figure 233 IP Address Conflicts: Case D



This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

Appendix E

IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Table 133 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID



Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have $2^8 - 2$ or 254 hosts.

A class “B” address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class “A” address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Table 134 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Table 135 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

Table 136 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 137 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.



Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

Table 138 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 139 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Table 140 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 141 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 142 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 143 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 144 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class “C” subnet planning.

Table 145 Class C Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets ([see Table 133](#)) available for subnetting.

The following table is a summary for class “B” subnet planning.

Table 146 Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix F

Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.



Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

For example,

`sys filter netbios config <type> <on|off>`

means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Appendix G

Log Descriptions

This appendix provides descriptions of example log messages

Table 147 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Table 148 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
SMT Login Successfully	Someone has logged on to the router's SMT interface.
SMT Login Fail	Someone has failed to log on to the router's SMT interface.
WEB Login Successfully	Someone has logged on to the router's web configurator interface.
WEB Login Fail	Someone has failed to log on to the router's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
FTP Login Successfully	Someone has logged on to the router via FTP.
FTP Login Fail	Someone has failed to log on to the router via FTP.

Table 149 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable

Table 149 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 150 Sys log

LOG MESSAGE	DESCRIPTION
Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"	This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

Log Commands

Go to the command interpreter interface (the *Command Interpreter Appendix* explains how to access and use the commands).

Configuring What You Want the ZyAIR to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyAIR is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Table 151 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
8021x	0, 1
access	0, 1, 2, 3
attack	0, 1, 2, 3
error	0, 1, 2, 3
icmp	0, 1
javablocked	0, 1, 2, 3
mten	0, 1
packetfilter	0, 1
remote	0, 1
tcpreset	0, 1
upnp	0, 1
urlblocked	0, 1, 2, 3
urlforward	0, 1
Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the ZyAIR (you must do this in order to record logs).

Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyAIR's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyAIR log category.

Use the `sys logs clear` command to erase all of the ZyAIR's logs.

Log Command Example

This example shows how to set the ZyAIR to record the error logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access

# .time                source                destination
notes
message
0|11/11/2002 15:10:12 |172.22.3.80:137
|172.22.255.255:137   |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
1|11/11/2002 15:10:12 |172.21.4.17:138
|172.21.255.255:138   |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
2|11/11/2002 15:10:11 |172.17.2.1           |224.0.1.60
|ACCESS BLOCK
    Firewall default policy: IGMP(set:8)
3|11/11/2002 15:10:11 |172.22.3.80:137
|172.22.255.255:137   |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
4|11/11/2002 15:10:10 |192.168.10.1:520
|192.168.10.255:520    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
5|11/11/2002 15:10:10 |172.21.4.67:137
|172.21.255.255:137   |ACCESS BLOCK
```

Appendix H

Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.

It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.

It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.

It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".

It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

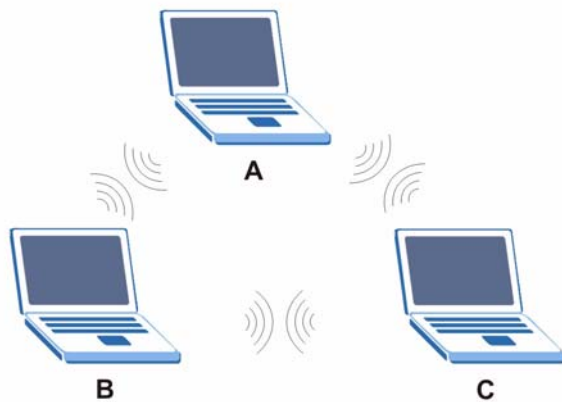
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

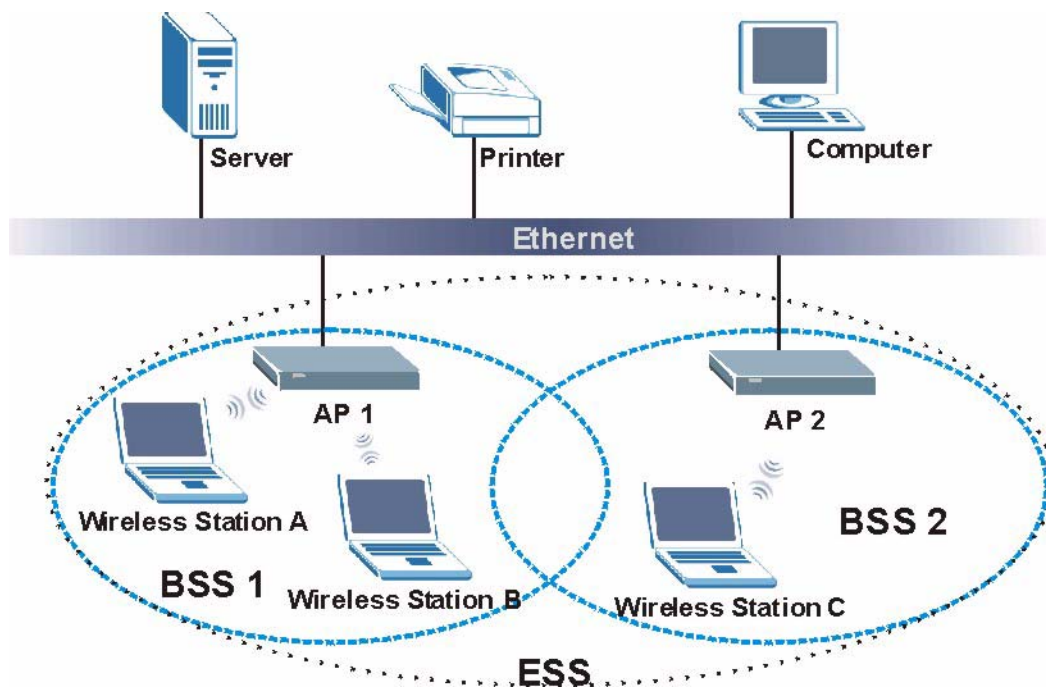
Figure 234 Peer-to-Peer Communication in an Ad-hoc Network



Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.

Figure 235 ESS Provides Campus-Wide Coverage

Appendix I

Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed.

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

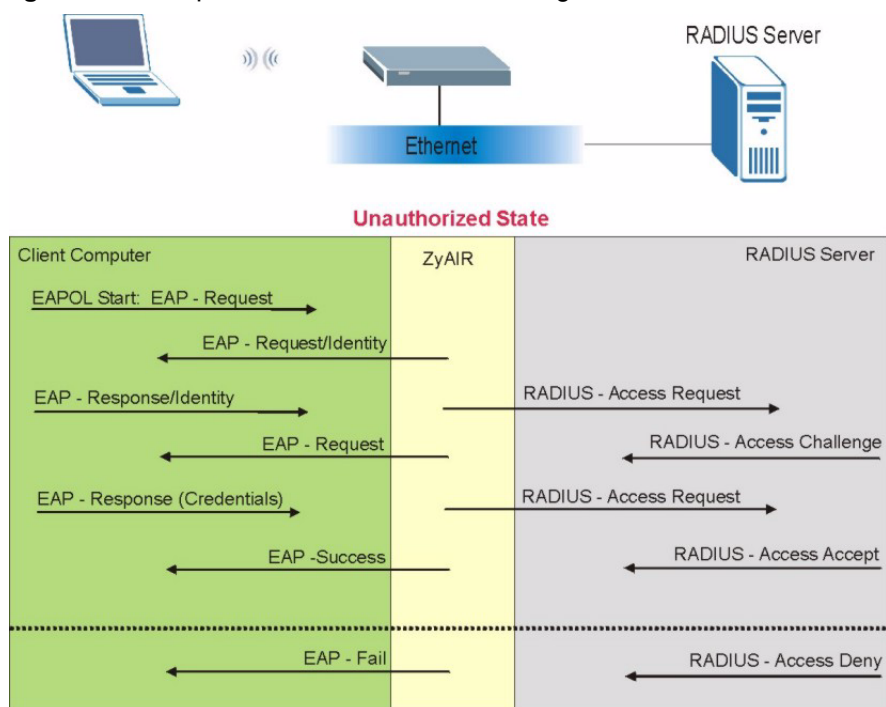
Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

Figure 236 Sequences for EAP MD5–Challenge Authentication

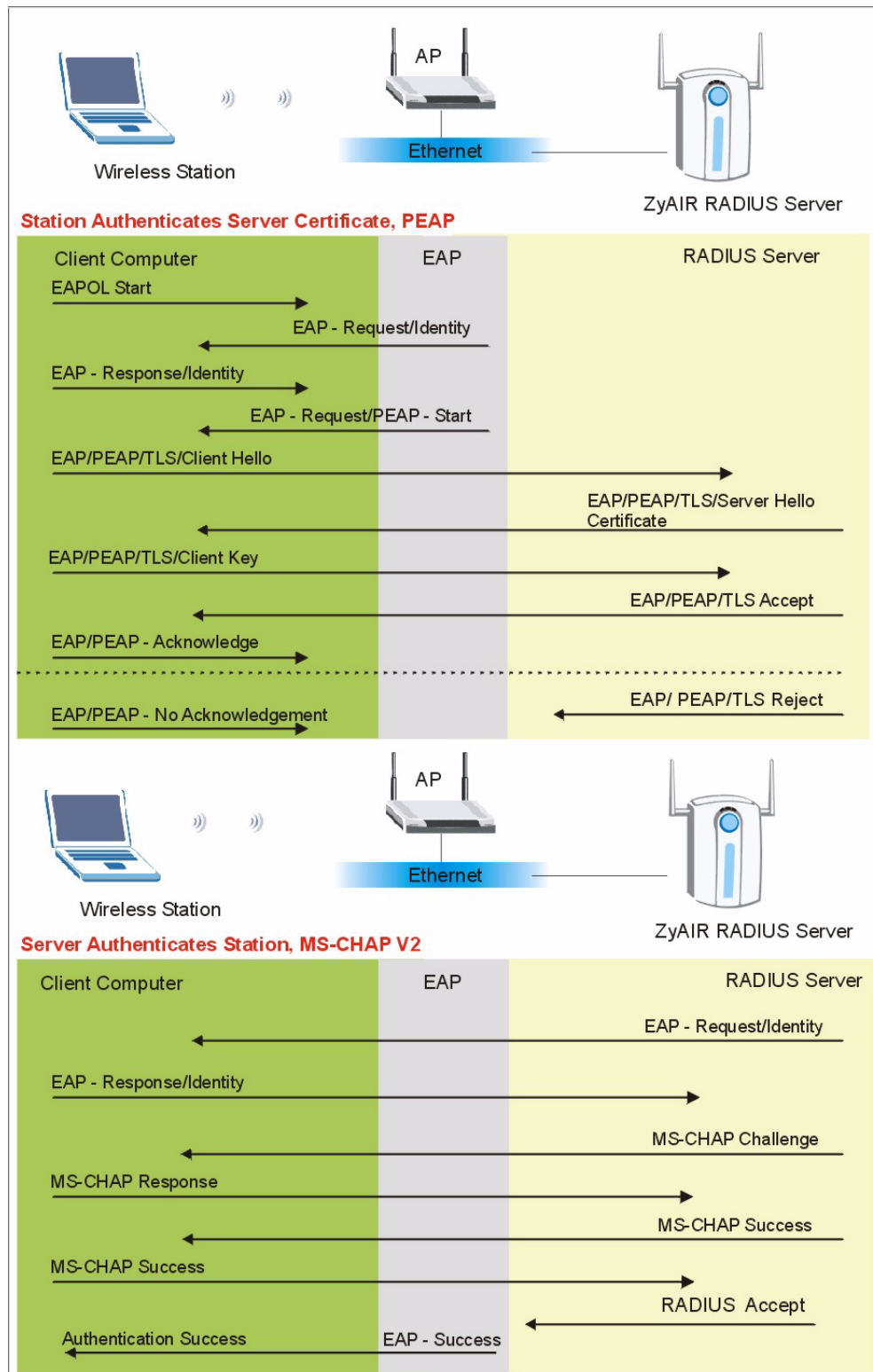


Mutual Authentication with Internal RADIUS server.

Microsofts Challenge-Handshake Authentication Protocol (MS-CHAP V2) is used to periodically verify the identity of the peer (station or other AP) using a three-way handshake.

The following figure depicts a typical wireless network with a ZyAIR RADIUS server for user authentication using PEAP (Protected EAP) and MS-CHAP V2.

The ZyAIR authenticates in two phases when it is acting as a RADIUS server:

Figure 237 Sequences for PEAP, MS-CHAP V2 Authentication

Appendix J

Types of EAP Authentication

This appendix discusses popular EAP authentication types.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of the authentication types.

Table 152 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

Appendix K

Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Connector Type

The ZyAIR is equipped with a reverse polarity SMA jack, so it will work with any 2.4GHz wireless antenna with a reverse polarity SMA plug.

Appendix L

Power Adaptor Specifications

Table 153 NORTH AMERICAN PLUG STANDARDS

AC Power Adaptor Model	AD48-1201200DUY
Input Power	AC120Volts/60Hz/0.25A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1950, CSA C22.2 No.234-M90)

Table 154 NORTH AMERICAN PLUG STANDARDS

AC Power Adaptor Model	DV-121A2-5720
Input Power	AC120Volts/60Hz/27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223-M91)

Table 155 EUROPEAN PLUG STANDARDS

AC Power Adaptor Model	AD-1201200DV
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950)

Table 156 United Kingdom PLUG STANDARDS

AC Power Adaptor Model	AD-1201200DK
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950, BS7002)

Table 157 Japan PLUG STANDARDS

AC Power Adaptor Model	JOD-48-1124
Input Power	AC100Volts/ 50/60Hz/ 27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	T-Mark (Japan Dentori)

Table 158 Australia and New Zealand plug standards

AC Power Adaptor Model	AD-1201200DS or AD-121200DS
Input Power	AC240Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	NATA (AS 3260)

Index

Numerics

802.1x [104](#)

A

Action for Matched Packets [202](#)
 Active [281](#)
 ActiveX [211](#)
 Allocated Budget [284](#)
 Alternative Subnet Mask Notation [398](#)
 Antenna
 Directional [421](#)
 Omni-directional [421](#)
 Antenna gain [420](#)
 Application-level Firewalls [178](#)
 Applications [42](#)
 Attack Types [184](#)
 Authen [284](#)
 Authentication [90](#)
 Authentication Protocol [283](#)
 Auto-crossover Ethernet/Fast Ethernet Interface [36](#)
 Auto-negotiating Ethernet/Fast Ethernet Interface [36](#)
 auto-negotiation [36](#)

B

Backup [248](#)
 backup [351](#)
 Basic Service Set [411](#)
 Brute-force Attack, [183](#)
 Brute-Force Password Guessing Protection [39](#)
 BSS [78](#), [411](#)
 Budget Management [364](#)

C

CA [418](#)
 Cable Modem [179](#)
 Call Control [363](#)
 Call History [364](#)
 Call Scheduling [372](#)
 Maximum Number of Schedule Sets [372](#)
 PPPoE [374](#)
 Precedence [372](#)
 Precedence Example [372](#)
 Certificate Authority [418](#)
 Channel [48](#)
 Channel ID [83](#)
 Collision [339](#)
 Command Interpreter [362](#)
 Community [329](#)
 Computer Name [258](#)
 Configuration [70](#), [242](#)
 Connection ID/Name [285](#)
 Content Filtering [210](#)
 Days and Times [210](#)
 Restrict Web Features [210](#)
 Cookies [211](#)
 Cost Of Transmission [291](#)
 CPU Load [339](#)
 Custom Ports
 Creating/Editing [202](#)

D

Data Encryption [90](#)
 Data encryption [48](#)
 Default [250](#)
 Denial of Service [179](#), [180](#), [326](#)
 Destination Address [194](#)
 DHCP [65](#), [70](#), [71](#), [73](#), [242](#), [243](#), [341](#)
 Diagnostic [347](#)
 Diagnostic Tools [338](#)
 Direct Sequence Spread Spectrum [410](#)

Distribution System [411](#)

DNS [165](#)

Domain Name [142](#)

DoS

Basics [180](#)

Types [181](#)

DS [411](#)

DSSS [410](#)

Dynamic DNS [65](#), [259](#)

Dynamic WEP Key Exchange [104](#)

DYNDNS Wildcard [65](#)

E

EAP [39](#)

EAP Authentication [101](#), [418](#)

ECHO [142](#)

Edit IP [282](#)

Encapsulation [281](#), [285](#)

Encryption [94](#)

Error Log [341](#)

Error/Information Messages

Sample [342](#)

ESS [79](#), [411](#)

ESS ID [48](#)

Ethernet Encapsulation [141](#), [280](#), [281](#)

Extended Service Set [79](#), [411](#)

Extended Service Set IDentification [83](#)

F

Factory LAN Defaults [70](#)

FHSS [410](#)

Filename Conventions [350](#)

Filter [264](#), [287](#)

Applying [324](#)

Example [321](#)

Generic Filter Rule [319](#)

Generic Rule [320](#)

NAT [323](#)

Remote Node [325](#)

Structure [313](#)

Finger [142](#)

Firewall

Access Methods [192](#), [326](#)

Address Type [201](#)

Alerts [196](#)

Connection Direction [195](#)

Creating/Editing Rules [199](#)

Custom PortsSee Custom Ports [202](#)

Firewall Vs Filters [188](#)

Guidelines For Enhancing Security [188](#)

Introduction [179](#)

Policies [192](#)

Remote Management [326](#)

Rule Logic [193](#)

Services [206](#)

SMT Menus [326](#)

Types [178](#)

When To Use [189](#)

Firmware File

Maintenance [244](#)

Fragmentation Threshold [81](#)

Frequency-Hopping Spread Spectrum [410](#)

FTP [65](#), [70](#), [140](#), [141](#), [142](#), [156](#), [160](#), [370](#)

Restrictions [370](#)

FTP File Transfer [357](#)

FTP Restrictions [156](#)

FTP Server [305](#)

G

Gateway [291](#)

Gateway IP Addr [286](#)

Gateway IP Address [276](#)

General Setup [49](#), [64](#), [258](#)

Global [136](#)

H

Hidden Menus [255](#)

Hop Count [291](#)

Host [67](#)

Host IDs [396](#)

HTTP [142](#), [178](#), [180](#)

I

IBSS [78](#), [411](#)

ICMP echo [183](#)

Idle Timeout [283](#), [284](#)

IEEE 802.1x [39](#)

IGMP [71](#), [72](#)

Independent Basic Service Set [78](#), [411](#)

Inside [136](#)
 Inside Global Address [136](#)
 Inside Local Address [136](#)
 Internet Access [274](#)
 ISP's Name [275](#)
 Internet access [264, 274](#)
 Internet Access Setup [275, 294](#)
 Internet Control Message Protocol (ICMP) [183](#)
 Internet Security Gateway [36](#)
 Introduction to Filters [312](#)
 IP Address [71, 74, 141, 143, 144, 266, 275, 286, 291, 341, 348](#)
 IP Address Assignment [286](#)
 IP Addressing [396](#)
 IP Classes [396](#)
 IP Pool [73, 266](#)
 IP Pool Setup [70](#)
 IP Ports [180](#)
 IP Spoofing [181, 184](#)
 IP Static Route Setup [290](#)
 IPSec VPN Capability [38](#)

J

Java [211](#)

K

Key Fields For Configuring Rules [194](#)

L

LAN Setup [70, 124](#)
 LAN TCP/IP [70](#)
 LAN to WAN Rules [195](#)
 LAND [181, 183](#)
 Link type [339](#)
 Local [136](#)
 Local User Database [120](#)
 Log Descriptions [406](#)
 Login Name [275](#)
 Logs [124, 232](#)

M

MAC Address [262](#)
 MAC Address Filter Action [113](#)
 MAC Address Filtering [112, 270](#)
 MAC Filter [112](#)
 MAC Filtering [39](#)
 Main Menu [255](#)
 Management Information Base (MIB) [162, 329](#)
 Many to Many No Overload [139](#)
 Many to Many Overload [139](#)
 Many to One [139](#)
 Metric [131, 154, 286, 291](#)
 Multicast [71, 74, 266, 287](#)
 My IP Addr [285](#)
 My Login [281](#)
 My Login Name [275](#)
 My Password [275, 281](#)
 My Server IP Addr [285](#)

N

Nailed-Up Connection [284](#)
 Nailed-up Connection [283](#)
 NAT [140, 141, 142, 286, 323](#)
 Applying NAT in the SMT Menus [294](#)
 Configuring [296](#)
 Definitions [136](#)
 Examples [302](#)
 How NAT Works [137](#)
 Mapping Types [139](#)
 Non NAT Friendly Application Programs [308](#)
 Ordering Rules [299](#)
 Server Sets [141](#)
 What NAT does [137](#)
 Network Address Translation (NAT) [294](#)
 Network Management [41, 142](#)
 NNTP [142](#)

O

One to One [139](#)
 Outside [136](#)

P

Packet Filtering [189](#)
Packet Filtering Firewalls [178](#)
Packets [339](#)
Password [67](#), [252](#), [253](#), [257](#), [275](#), [329](#)
Period(hr) [284](#)
Ping [347](#)
Ping of Death [181](#)
Point-to-Point Tunneling Protocol [129](#), [142](#)
POP3 [142](#), [180](#)
Port Numbers [142](#)
PPPoE Encapsulation [278](#), [280](#), [283](#), [284](#)
PPTP [142](#)
Private [154](#), [287](#), [291](#)

Q

Quick Start Guide [44](#)

R

RADIUS [39](#), [100](#)
RAS [341](#)
Rate
 Receiving [339](#)
 Transmission [339](#)
Related Documentation [32](#)
Rem Node Name [281](#)
Remote Authentication Dial In User Service [39](#)
Remote Management
 Firewall [326](#)
Remote Management and NAT [157](#)
Remote Management Limitations [156](#), [370](#)
Remote Node [339](#)
Remote Node Filter [287](#)
Reports [236](#)
Required fields [255](#)
Reset Button [37](#)
Restore [248](#)
Restore Configuration [355](#)
Restrict Web Features [211](#)
RF signals [410](#)
RIP [71](#), [287](#)
 Version [287](#)
Roaming [84](#)

Example [84](#)
Requirements [85](#)
Route [282](#)
RTS Threshold [80](#)
Rules [192](#), [195](#)
 Checklist [193](#)
 Creating Custom [192](#)
 Key Fields [194](#)
 LAN to WAN [195](#)
 Logic [193](#)

S

Saving the State [185](#)
Schedule Sets
 Duration [373](#)
Schedules [284](#)
Security Parameters [90](#)
Security Ramifications [194](#)
Server [139](#), [140](#), [275](#), [281](#), [296](#), [298](#), [300](#), [301](#), [303](#), [304](#), [305](#)
Server IP [281](#)
Service [194](#)
Service Name [284](#)
Service Set [83](#)
Service Type [202](#), [275](#), [281](#)
Services [141](#), [142](#)
setup a schedule [373](#)
SMT Menu Overview [253](#)
SMTP [142](#)
Smurf [183](#), [184](#)
SNMP [41](#), [142](#), [161](#)
 Community [330](#)
 Configuration [329](#)
 Get [329](#)
 GetNext [329](#)
 Manager [162](#), [328](#)
 MIBs [162](#), [329](#)
 Set [329](#)
 Trap [329](#)
 Traps [330](#)
 Trusted Host [330](#)
Source Address [194](#), [201](#)
SSL Passthrough [38](#)
Stateful Inspection [178](#), [179](#), [185](#)
 Process [185](#)
Static Route [152](#)
STP (Spanning Tree Protocol) [38](#)
SUA [140](#), [142](#)
SUA (Single User Account) [140](#)
Subnet Mask [71](#), [74](#), [201](#), [266](#), [276](#), [286](#), [291](#), [341](#)

Subnet Masks [397](#)
Subnetting [397](#)
SYN Flood [181](#), [183](#)
SYN-ACK [182](#)
Syntax Conventions [33](#)
Syslog [203](#), [206](#)
System
 Console Port Speed [341](#)
 Diagnostic [346](#)
 Log and Trace [341](#)
 System Information [340](#)
 System Status [338](#)
 Time and Date [365](#)
System Information [340](#)
System Information & Diagnosis [338](#)
System Maintenance [338](#), [340](#), [351](#), [354](#), [355](#), [357](#), [359](#),
 [362](#), [363](#), [364](#), [366](#)
System Name [64](#), [259](#)
System Timeout [157](#), [371](#)

T

TCP Security [187](#)
TCP/IP [74](#), [180](#), [181](#), [317](#), [323](#), [347](#), [370](#)
TCP/IP filter rule [317](#)
Teardrop [181](#)
Telnet [158](#), [369](#)
Telnet Configuration [369](#), [370](#)
Telnet Under NAT [370](#)
TFTP
 Restrictions [370](#)
TFTP File Transfer [359](#)
TFTP Restrictions [156](#)
Three-Way Handshake [182](#)
Time and Date Setting [365](#)
Time Setting [68](#)
Time Zone [366](#)
Timeout [277](#), [278](#), [284](#)
Trace Records [341](#)
Traceroute [184](#)
Traffic Redirect [40](#)
Trigger Port Forwarding [310](#)
 Process [148](#)
Troubleshooting
 Accessing ZyAIR [377](#)
 Ethernet Port [376](#)
 Start-Up [376](#)

U

UDP/ICMP Security [187](#)
Universal Plug and Play (UPnP) [168](#)
Upload Firmware [357](#)
Upper Layer Protocols [187](#), [188](#)
URL Keyword Blocking [211](#)
Use Server Detected IP [261](#)
User Authentication [93](#)
User Name [66](#), [260](#)
User Profiles [292](#)
User Specified IP Addr [261](#)

V

Valid CI Commands [363](#)
VPN [129](#)

W

WAN DHCP [347](#)
WAN Setup [262](#)
WAN to LAN Rules [195](#)
Web [157](#)
Web Configurator [44](#), [46](#), [179](#), [188](#), [194](#), [327](#)
Web Proxy [211](#)
WEP [48](#), [90](#)
WEP Encryption [39](#), [92](#), [96](#)
Wi-Fi Protected Access [37](#)
Wireless Client WPA Supplicants [97](#)
Wireless LAN [268](#), [410](#)
Wireless LAN Setup [268](#)
Wireless Security [88](#)
Wizard Setup [48](#), [49](#), [50](#)
WLAN [410](#)
WPA [37](#), [93](#)
WPA with RADIUS Application [97](#)
WPA-PSK Application [94](#)
www.dyndns.org [261](#)

Z

ZyAIR LED [37](#)
ZyNOS [351](#)

ZyNOS F/W Version [351](#)

ZyXEL's Firewall
Introduction [179](#)